AD-A211 137

VOL. V

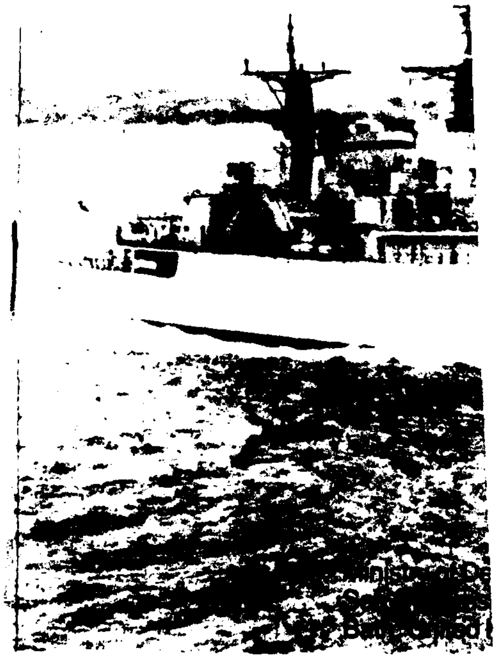
Proceedings

Seventh Ship Control Systems Symposium

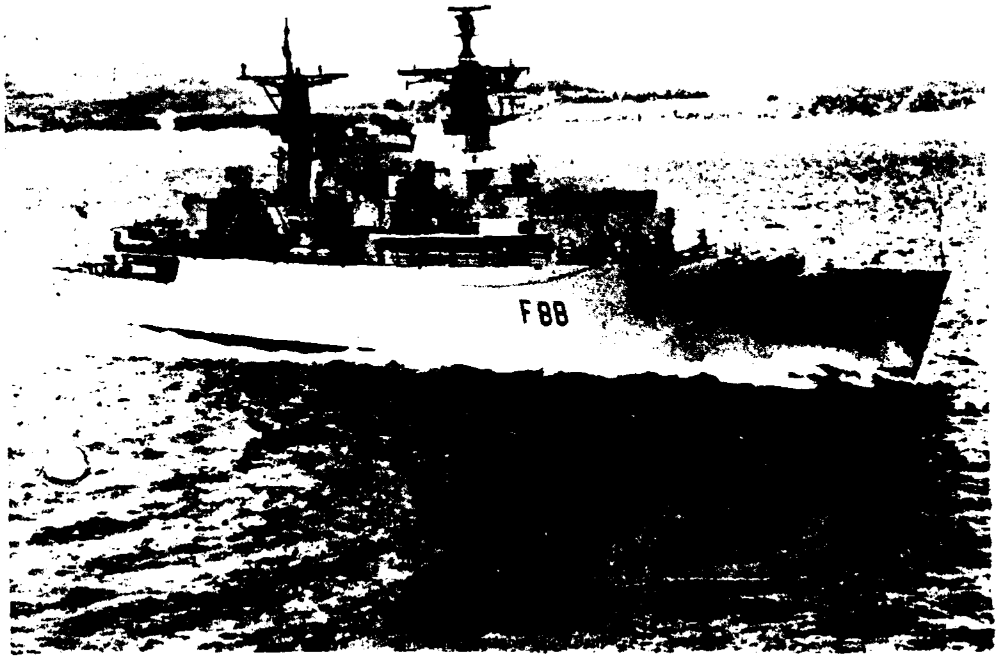
24 – 27 September 1984
Bath, United Kingdom

Volume 5

Vol 1	BR 94196
Vol 2	BR 94197
Vol 3	BR 94198
Vol 4	BR 94199
Vol 5	BR 94200
Suppl Index	BR 94201



1984
Bath, UK



PUBLICATION INFORMATION

These papers were printed just as received from the authors in order to ensure their availability for the Symposium.

Statements and opinions contained therein are those of the authors and are not to be construed as official or reflecting the views of the United Kingdom Ministry of Defence.

Authors have given permission on behalf of themselves and/or their employers for the United Kingdom Ministry of Defence to publish their paper(s) in the Proceedings of the Seventh Ship Control Systems Symposium. No material contained within these Proceedings may be reproduced without the prior permission of the publishers.

Requests for further information regarding the Proceedings and the Symposium should be addressed to:

B BLOCK. MINISTRY OF DEFENCE (PE). FOXHILL. BATH. BA1 5AB. UK:
ATTENTION: ADMC.

INDEX

AN INTEGRATED AND SURVIVABLE DAMAGE CONTROL SYSTEM FOR MODERN WARSHIPS

by L.B. Mayer
and J.M. Kuran
Ginge-Kerr Canada Ltd.

ABSTRACT

Recent events have reinforced the need for a comprehensive information/control system for damage control on warships. This paper examines the requirements for such a system and describes the system philosophy selected for use on the new Canadian Patrol Frigate. Integration and survivability requirements are discussed as well as the cost implications of various solutions to the problem.

INTRODUCTION

Shipboard damage control consists, in broad terms, of the monitoring and surveillance of a warship's integrity prior to sustaining damage; the reporting of damage to the damage control organisation; and the coordinated directed response to damage by the damage control organisation in a timely and efficient manner thereby ensuring the continued availability, mobility and survivability of the fighting platform. When one considers that damage can consist of any combination of fire, flood, smoke and under certain circumstances NBC contamination as well as physical damage to systems provided to combat the damage, it becomes readily apparent that the solution is not trivial.

Historically, monitoring and surveillance have depended on a number of independant stand-alone monitoring systems (such as fire detection and bilge level alarms) and on the ability of damage control roundsmen to detect and report abnormal conditions. Information from roundsmen, stand-alone systems and Damage Control Teams was passed verbally via messengers or by sound powered telephone sets to the Damage Control Headquarters and to Section Bases. This information was then manually collated by plotters with incidents being logged and displayed on passive state boards. The very nature of the information gathering process created significant time delays which prevented the rapid response often necessary to contain and control an incident.

The effectiveness of this method of operation is also extremely dependant on ship's personnel remaining aware of the changing damage control situation. Due to the number of different personnel involved in the reporting process the global picture necessary to respond efficiently and effectively is often incomplete particularly if smoke conditions force personnel to evacuate a section of the ship.

Based on the advances in micro-electronic technology over the last decade, Ginge-Kerr Canada developed a proprietary multiplexing system (Fire-Scope) which permitted an economical solution to providing an integrated and survivable Damage Control system. This integrated system philosophy was proposed to and selected by Saint John Shipbuilding and Dry Dock for implementation on the Canadian Patrol Frigate (CPF) currently being designed and constructed for the Canadian Navy.

CPF FITTED DAMAGE CONTROL SYSTEMS

The CPF is a CODOG frigate of approximately 4200 tonnes displacement designed primarily for an ASW mission. Consistent with current Canadian Navy philosophy it is highly automated in order to minimize manning requirements and improve threat reaction times. With the increasing sophistication (and concurrently cost) of such a vessel there has been a growing awareness of the need to improve the Damage Control capabilities. As a result, the number of systems and level of automation of Damage Control functions on the CPF far exceed what has been installed on any recent warship of this size.

The overall fitted Damage Control systems on the CPF can be broken down into four major subsystems as follows:

- Fire Detection and Suppression System
- Firemain Status and Control System
- Ventilation Status and Control System
- Liquid Level Management System

Fire Detection and Suppression System. The fire detection and suppression system monitors the whole ship for fire. There are approximately 400 smoke and heat detectors fitted throughout the vessel grouped into 75 defined damage control zones. Alarm indication is provided both at Damage Control headquarters and at the Quartermasters position for those situations when the ship is alongside with only a harbour watch on duty.

Main and reserve banks of halon 1301 are provided to protect 44 electronic and high value compartments throughout the ship. Each halon system will discharge automatically if two fire detectors in a compartment go into alarm and can also be manually released from DC headquarters by the operator.

A centralized Aqueous Film Forming Foam (AFFF) proportioning system is provided to serve 13 compartments. Release of AFFF can be effected from DC headquarters or from local control points at each protected compartment. The system automatically starts proportioner pumps, opens distribution valves and selects the correct proportioner based on the required flow rate.

Firemain Status and Control System. The seawater firemain is fed by 7 firepumps and supplies water to fire hydrants throughout the ship, the NBC prewet system and to dedicated sprinkling systems in 18 compartments in the ship. The sprinkling systems are automatic in operation with indication at both DC headquarters and the aft section base of initiation of sprinkling. Additionally,remote manual control from DC headquarters and the aft section base is provided to permit the operator to either override or initiate pre-flooding of magazines. Due to the requirements for survivability the firemain is heavily valved to permit isolation of individual sections within the ship. The status of approximately 60 isolation valves in the system is displayed to provide the operator with an instantaneous overview of system configuration.

The seawater system also drives the main compartment eductors and hence bilge flooding alarms for 18 distinct areas are displayed for the operator.

Ventilation Status and Control System. The ventilation systems on a warship are inextricably linked with the damage control function both due to the requirement to maintain citadel overpressures under NBC conditions and to isolate fires and prevent smoke propagation throughout the ship. The ventilation control system is interlocked with the halon 1301 release control so that the correct fans are automatically stopped prior to the release of halon.

The damage control operator is provided with the capability to automatically select a full NBC gastight configuration for the ship with a single command. The control system automatically selects the correct alignment of ventilation fans, dampers and NBC filtration units as well as alerting the operator of any manually controlled hatches, doors or dampers which are not in the correct position. In order to provide the operator at DC headquarters with this capability the system must monitor and control the following:

40	ventilation fans
40	remote controlled dampers/valves
4	NBC filtration units
10	citadel pressures
15	citadel doors
140	manually operated dampers/valves

Liquid Level Management System. The liquid level management system provides centralized control and monitoring of the ships tanks including fuel oil, helofuel, fresh water and ballast tanks. The system provides a fully automatic refuelling capability by monitoring tank levels and automatically closing filling valves to each tank. Total tank quantities are provided for each of the four tank groups as well as individual values for each tank in order to permit stability calculations. Remote manual control is provided for tank valves and transfer pumps to permit counter flooding by the operator should it be necessary.

SYSTEM INTEGRATION

Overall the Damage Control system has to monitor and control approximately 800 points distributed throughout the whole ship from the keel through the superstructure. The damage control team in DC headquarters must be provided with an overall global summary of the ship's integrity and instantaneous indication of any damage that may occur. This data must be presented in a comprehensive and cohesive fashion to permit the damage control officer to make an intelligent assessment of the nature and extent of the damage, and means must then be provided for the damage control team to take the necessary corrective action.

In order to achieve this goal, the initial concept was to provide hard mimic panels for each of the four subsystems. Each mimic panel is between half to one square meter in size and provides a geographical depiction of the ship along with the relevant system schematic. Each alarm and/or control point is identified by an LED pushbutton located on the mimic in the same location as it is physically on the ship. Control by the operator is exercised by depressing the LED/pushbutton for the relevant location and simultaneously selecting the desired executive action from a group of command pushbuttons (such as valve open/close, release, start, etc.).

The requirement for coincident actuation of two physically separate pushbuttons in order to initiate an action minimizes the possibility of inadvertent activation of any system. Provision of geographically similar ship's mimic provides the damage control team with a clear picture of the ship's overall damage state and replaces the traditional manually updated state boards.

The mimics are mounted in a wrap around console which is manned by the damage control operator. The console is designed to ensure that all pushbuttons are within easy arm reach of the seated operator. The cla.ity and size of each mimic provides the DC officer, who is seated at a desk behind the operator, with an instantaneous summary of the ships condition.

Each of the four subsystems has its own independant central control unit which is responsible for data gathering via a multiplexing loop, data manipulation as necessary, display and command telemetry. Provisions are made to transfer information between processors as necessary and to interface with the machinery control system. Optical couplers are provided to ensure galvanic decoupling between the systems.

Between the time that the system was originally designed and specified, advances in technology have resulted in the availability on the market of shock qualified colour display screens. This availability coupled with the decision to install a colour CRT based machinery control system (SHINMAC) on the CPF (1) has led to the consideration of the use of colour CRT's for damage control as well. Although no final decision has been made on this option, it does offer significant advantages both in the amount and method of data presentation as well as in the area of hardware commonality and logistics support.

The basic system configuration does not change if CRT's are used. Each of the four subsystems would retain its own loop control unit which would remain responsible for the operation of the loop. Data would be transfered from each control unit to the CRT graphics driver to be displayed on a dual CRT console. The design of the man/machine interface including display, command selection and control interaction would be in accordance with the guidelines specified for SHINMACS.(2)

The CRT based system has the added advantage that it provides the capability to plug a portable CRT unit into the system at a remote location should the interior of the ship become intenable due to smoke or damage.

SURVIVABILITY

The requirements for damage survivability of a damage control system are inherent. The availability of the system must be guaranteed during and especially subsequent to damage suffered by the ship and consequently by various parts of the control system. However, redundancy is to be minimized due to cost considerations.

The Fire-Scope system was designed within the constraints of these requirements. The requirements for flexibility and adaptability of the control system dictated the use of computer based technology, capable of self-testing and fault diagnosis. The control network, requiring operation in the electrically noisy and otherwise hostile marine environment dictated the use of multiplexing techniques capable of analogue and digital (numerical) filtering. The need for survivability caused by damage or failure dictated the use of a loop wiring configuration, thereby eliminating the need for cabling redundancy. The various standard addressed multiplexed systems, not having the sophistication of weapons type data buses, had to be discarded due to their susceptibility to induced noise end high radiated emission levels. Consequently, a proprietary communication network has been designed. The selected protocol operates at a sufficiently low frequency to permit the use of conventional wiring (as opposed to coaxial cabling), while still producing significantly high information update rates. The Fire-Scope system provides for a complete system update (consisting of the centralized gathering of the status of monitored field devices, the processing of this information and the subsequent control signal actuation) in approximately one second for as many as 500 field devices per control unit.

Status and control signals are received and transmitted in both clockwise and counter-clockwise direction on the loop in order to render the system immune to first failure conditions, while permitting the diagnosis and location of faults. The use of the so called "clothes-line" data bus has been eliminated in favor of point-to-point analogue filtering and signal regeneration. This technique has resulted in considerably lower signal power requirements, thereby reducing emission to an extremely low level. Additionally, susceptibility to externally induced noise has been substantially reduced.

The control units, by virtue of the fact that they are computer based, are capable of self-testing and fault diagnosis. This feature has been extended to the testing and health monitoring, by the central control unit, of all the distributed remote electronic devices. Consequently, the probability of a device being unavailable when required, is virtually eliminated.

Each control unit is provided with a watch-dog supervisory circuit, failure of which results in an audible and visual annunciation. However if a control system failure should occur during fire fighting or action conditions, the Damage Control Operator would still have to contend with the system MTTR, during which time, Damage Control would have to revert to local manual control. While this would be acceptable under normal conditions, it would present a serious problem when the Damage Control System is most required. Furthermore, should the Machinery Control Room /Damage Control Headquarter become untenable due to damage, the sophistication offered by the computerized control systems would be wasted. Consequently, for selected Damage Control functions, complete control and monitoring redundancy is provided from two physically separate locations.

Having this redundancy, should a controller failure occur at the Primary location, the Reversionary controller shall automatically take over, without interruption or loss of information. Additionally, operator monitoring and control is always available at both locations, inspite of a failure of either control unit. Thus the "down-time", due to repair requirements of a failure, are non-existent.

A prototype Evaluation Unit of thisprime/Reversionary configuration has successfully passed functional and environmental tests as required by MOD(N) at the Royal Navy Test Establishment, West Drayton, in March 1984.

The reliability block diagram for this Prime/Reversionary System is the two controllers arranged in active redundancy, that is in parallel, with both controllers operating but only one required to be "On Line" for total system operation.

If	R(D)	Dual Controller arrangement reliability
	R(P)	Primary Controller reliability
	R(R)	Reversionary Controller reliability

then the reliability mathematical model for this system is:

$$\begin{aligned} R(D) &= R(\text{mission success with Primary On Line})\ R(P) \\ &= R(\text{mission success with Primary Failed})(1-R(P)) \end{aligned}$$

but R(mission success with Primary On Line) is unity, since any one Controller can support the full requirements of the system,

and R(mission success with Primary Failed) is now equivalent to the reliability of the Reversionary Controller

$$\text{thus } R(D) = R(P) + R(R)(1-R(P)).$$

Since the two Controllers are identical, then:

$$R(P) = R(R) = R$$

which is the reliability of either Controller,

$$\begin{aligned} \text{therefore } R(D) &= R + R(1-R) \\ &= R(2-R) \end{aligned}$$

Clearly, from the above equations, the reliability of a Prime/Reversionary system is greater by the factor (2-R) than the reliability of a single Controller System.

In terms of actual numbers:

Mission length = 90 days (2160 hours)
MTBF of a Control Unit = 7200 hours

Assuming failure distribution to be exponential a Control Unit reliability can be calculated from:

$$\begin{aligned} R &= \exp(-\text{Mission Length}/\text{MTBF}) \\ &= \exp(-2160/7200) \\ &= .741 \end{aligned}$$

and the reliability of the Prime/Reversionary system is:

$$\begin{aligned} R(D) &= R(2-R) \\ &= .741(2-.741) \\ &= .933 \end{aligned}$$

his translates to a dual system MTBF as follows:

$$\begin{aligned}\text{MTBF (dual system)} &= -\text{Mission Length}/\ln R(D)\\ &= -2160/\ln(.933)\\ &= 31{,}000 \text{ hours}\end{aligned}$$

Therefore the MTBF of a Prime/Reversionary System increases by a factor of 4.3 over a single Controller System.

The facility to request Control Position is provided at both DC headquarters and the AFT section base. The Control Position change-over function is arranged to ensure safe, stable and disciplined transfer of control. The On-Line, Standby or Failed status of both controller systems is displayed at both positions.

INSTALLATION COSTS

During the initial phases of the system concept design, a preliminary study was undertaken to determine the impact on the amount of ships cabling necessary to implement such a system. The system as described earlier monitors and controls approximately 800 points distributed throughout the whole ship. Of these 800 points some 700 are discrete and 100 analogue.

A conventional hardwired system was blocked out on a representative frigate arrangement plan. Although any number arrived at without doing detailed cable routing drawings must be considered an estimate, initial indications were that approximately 10,000 meters of various kinds of multicore cable would be required to wire the system. As a comparative example in U.S.N. study, Blackwell estimated that in a conventional DDG 47 class ship the Damage Control network required approximately 56,000 meters of cabling (3).

Multiplexing signals can significantly reduce the amount of cabling required. Blackwell (4), Carruthers (5) and many others have addressed this topic using conventional multiplexing architectures such as SDMS and SHINPADS with estimated cable savings varying depending on the application. One of the drawbacks in such an approach is that these are high speed data buses which require sophisticated bus access electronics. As a result they still require hardwiring of sensors/actuators to distributed electronic interfaces as shown in figure 1.

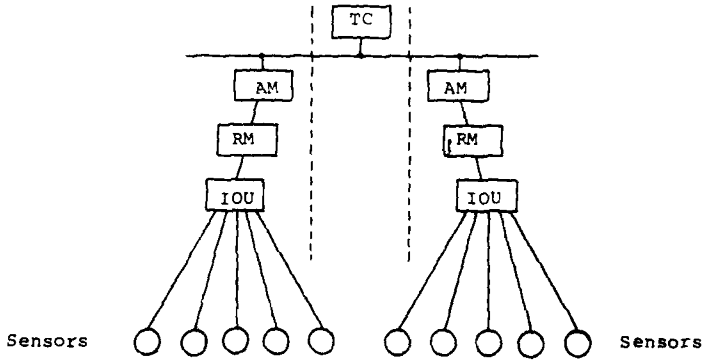


FIGURE 1. SERIAL DATA BUS CONFIGURATION

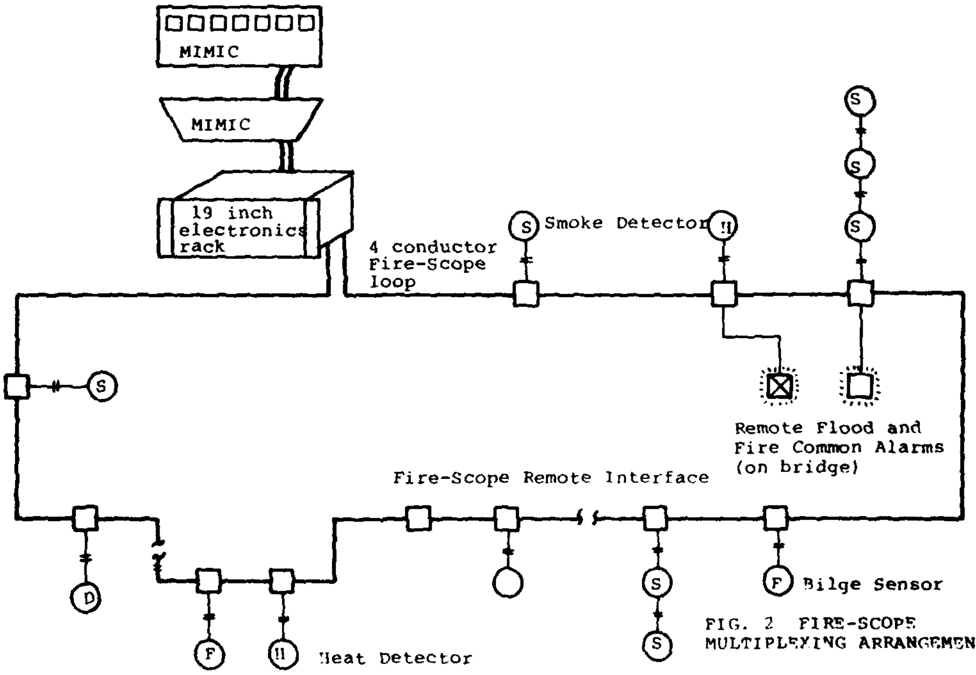

MIMIC
MIMIC
19 inch electronics rack
4 conductor Fire-Scope loop
S
Smoke Detector
H
S
S
S
S
Remote Flood and Fire Common Alarms (on bridge)
Fire-Scope Remote Interface
D
F
H
Heat Detector
S
S
F
Bilge Sensor

FIG. 2 FIRE-SCOPE MULTIPLEXING ARRANGEMENT

Since damage control sensors are so widely scattered throughout the ship this would require approximately 4600 meters of hardwiring in addition to the bus cables. As a comparison, Blackwell estimated a savings of 30 percent for the DDG 47 (6). Considering the low data transmission rate requirements of the Damage Control System, this would appear to be an expensive and inefficient use of a sophisticated data bus.

The Fire-Scope multiplexing loop approach strings a single 4 core cable throughout the ship picking up sensors/actuators in each compartment as it passes. This approach as shown in figure 2 would require approximately 1500 meters of loop wire and 300 meters of hardwiring for short stub runs where necessary.

The Fire-Scope has tne added advantage that power for the electronic interface cards and sensors is provided via the loop cable thereby eliminating the need for extensive power distribution wiring. The overall savings in cabling without addressing comparative hardware costs are summarized in table 1.

Table 1. Comparison of Cabling Requirements

System Type	Cable Length (m)	Cable Weight Tonnes	Cable Installation Cost (115 US/m)
Hardwired	10,000	7.5	1,150,000
Serial Bus	4,600	3.5	529,000
Fire-Scope	1,800	1.0	207,000

CONCLUSION

The integrated Damage Control system as proposed for the CPF provides the ships damage control organisation with a comprehensive display and control capability surpassing any previously provided on warships of this size. The system, due to the structure of its multiplexing methods and multiple control units, achieves this objective in an economical fashion while offering at the same time the high level of survivability necessary for a warship system which is required to operate under the most extreme cases of damage to the ship.

REFERENCES

(1) R. Khan and P. Eich, "Canadian Patrol Frigate Machinery Control System" Proceedings of the Seventh Ship Control System Symposium.

(2) Human Engineering Design Requirements for SHINMACS Machinery Control Consoles, Part III Console Displays and Operation, DCIEM Technical Report 81-R-18, Toronto 1981.

(3) L.M. Blackwell "Shipboard Data Multiplex System, Engineering Development Aspects and Applications," Proceedings of the Sixth Ship Control System Symposium, Ottawa, Ont., 1981 P. D23-11.

(4) Ibid.

(5) J.F. Carruthers (Cdr C.F.), "SHINPADS - A New Ship Integration Concept," Naval Engineers Journal, April 1979.

(5) Blackwell, op.cit., P-D3-11.

SOFTWARE FOR ROYAL NAVY SHIP CONTROL SYSTEMS

by Martin P.G. O'Byrne
CAP Scientific Ltd

ABSTRACT

The Royal Navy will introduce full digital ship plant control systems in the type 23 Frigate and the type 2400 Submarine. CAP Scientific are responsible for the software for these systems. This paper addresses the problems associated with the development of the software describing the methodologies employed and the discipline required for development of such systems. Reliability and commonality are considered.

INTRODUCTION

The next generation of Royal Naval Frigates - the type 23 - will be the first ship of the Royal Navy to have digital electronic control of the propulsion machinery. CAP Scientific are responsible for producing the software for the control system. The hardware will be the D86 system produced by Vosper Thornycroft Controls - this is a militarised family of hardware modules based on the Intel 8086 microprocessor. CAP Scientific are working under contract to Vosper Thornycroft. A similar digital system for surveillance will be used in the new Type 2400 submarine.

This paper addresses aspects of the software development for:

- T23 Machinery Control and Surveillance (MCAS)
- T23 Main Electrical Power System (MEPS)
- T2400 Surveillance

The areas discussed are:

- Specification of the Requirement
- Design Methodology
- Software Development
- Software Testing
- System Reliability Considerations
- A Practical Problem
- The Payoff
- Future Role of Software in Ship Control Systems

SPECIFICATION OF THE REQUIREMENT

The Problem

The ideal way to produce any system is to know exactly what is required before the start of design. We all realise that this is not true in the real world. The requirement-definition loop involves typically many people from many organisations. Consequently definition of the requirement in detail is usually not achieved until a significant part of the overall design is complete. Because of this factor we usually find that inconsistencies in the requirement are often not detected until this late stage. More errors result as a consequence of incorrect specification than at any stage of the development phase of a system. If these errors are not detected until late in the programme the cost implications can be very painful. Experience has shown that the cost difference between making a change during the specification phase and implementing the change post development can be a factor of 20:1. If a change in requirement post development is identified then this cost can be allowed for. However, if the "change" comes about because of late specification of the actual requirement or amplification of a stated requirement then the resultant increase in cost is very difficult to plan in and usually results in both time and cost overrun.

No specification is ever free of errors. The cost of errors at various stages of development is shown in Figure 1.

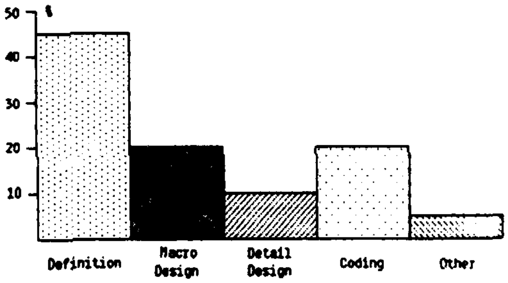


Figure 1 Software Fault Profile

How can they be minimised? Some major problems usually encountered in producing specifications are that they:

i) are incomplete
ii) are ambiguous
iii) don't show interdependencies
iv) are difficult to understand
v) are difficult to maintain.

The production of any specification requires a special discipline and the above points and others must be specifically addressed.

The technique we selected to attempt to overcome these problems is that advocated by Tom De Marco (1). A brief outline of the technique is given below. We then indicate how suitable this technique proved to be for our application.

The Technique

Elements of the Structured Specification. The main aim of De Marco's Structured Analysis method is to produce a readily maintainable Functional Specification document which has no internal redundancy. In order to achieve this aim the technique requires that:

- problems of size of specification are dealt with using an effective method of partitioning;
- graphics are used wherever possible;
- one differentiates between logical and physical considerations of the system;
- one builds a logical system model so that the user can gain familiarity with system characteristics before implementation.

In order to assist with the analysis task, the technique supplies three types of analysis phase tool; i.e.

a) The Data Flow Diagram (DFD) which is a network representation of a system. It portrays the system in terms of its component processes and the connections between those processes.

The graphical convention for DFDs is shown in Figure 2.

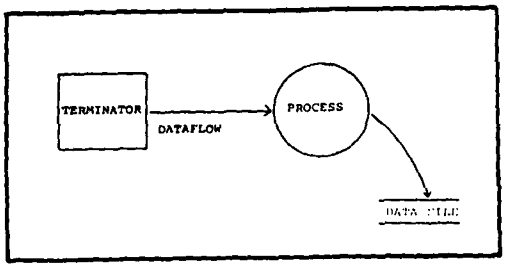


Figure 2 DFD Convention

The elements that make up a DFD are:-

- the dataflow, a vector indicating a well-defined information flow;
- the process, which transforms incoming dataflow(s) into outgoing dataflow(s);
- the terminator, which is a sink or source of data that is external to the system;

- the file which is a temporary repository of data.

Using these elements the DFD shows the major decomposition of function and defines all the interfaces between processes.

b) The Data Dictionary (DD), which complements the DFDs by documenting each of the interface dataflows and data files on any of the diagrams. It is a complete set of formal definitions which are accomplished by declaring the component data elements of each dataflow or data item and the relationships that apply among them.

Thus, so far, the system specification can be documented using network diagrams (DFD) which represent the system as a connected set of component processes and a data dictionary (DD) defining all the connections between declared components. To complete the model requires:

c) The Process Specification (PS), which specifies the component processes. In fact the DFDs are successively partitioned to lower levels of detail until a "primitive" process is characterised. Every one of these primitive processes is described by a Process Specification which defines the transformation that converts incoming data to outgoing data.

The PS is written using a "Structured English" which follows simple, but formal rules of layout and comprises a set of keywords which help to describe the structure of the process. Where it is appropriate, the PS can employ Decision Tables or Decision Trees as an alternative means of specifying the process.

These three analysis-phase tools allow the full documentation of the model of the required system. The interaction between this documentation set is shown in Figure 3.

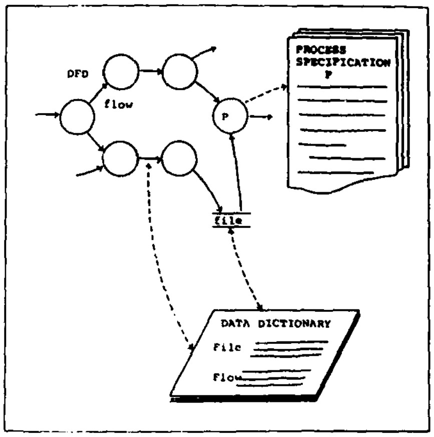


Figure 3 Documentation Set

Suitability of the Technique

A number of advantages have been found in using this structured analysis method compared with more traditional methods of specification. These include:

- The structured partitioning of the specification.
- The removal of internal redundancy.
- The rigorous definition of all interfaces.
- The formal definition of system functions.

Combined, the factors listed above go a long way to alleviating the problems, often found during the specification phase of a project, which we have already discussed.

The structured partitioning of the specification and removal of internal redundancy leads to a specification document which is both unambiguous and concise. In addition the strict use of Data Flow Diagrams, Data Dictionaries and process specifications must fully account for all data flows in a system and hence produce a complete specification, which indicates all interdependencies within the system.

The Analysis document produced using the De Marco technique appears very different from documents produced using more traditional methods. However, the combination of graphical presentation and a formal specification language does provide a clear and concise statement of the specification. There is of course a learning cost while the technique is learned by those receiving such a document for the first time but once a reader is familiar with the De Marco technique, the Analysis document is easily understood.

The maintainability of the specification document is enhanced by the lack of internal redundancy. More importantly, the generation and maintenance of Data Flow Diagrams and Data Dictionaries are ideally suited to automated techniques, which not only aids the maintainability of the document, but also eases the preparation of the first issue.

This structured analysis method is, as yet, imperfect and requires further development. Most importantly the current method does not adequately cover initialisation and failure modes which are both of considerable importance in a real-time system. However, the experience to date is that the use of structured Analysis techniques offer considerable advantages, particularly when backed up by automated development techniques and can considerably ease the process of producing a complete specification of a real-time system.

DESIGN METHODOLOGY

The Problem

Given an adequate requirement specification we must then take special account of those factors which will affect the design methodology. These include:

i) The systems perform a critical control function affecting the operational performance of the vehicle. MCAS controls the ship's propulsion plant while MEPS controls the ship's electrical power. A highly reliable system is required.

ii) The system involves the use of distributed processors - twenty in the case of MCAS. The software will likewise be distributed and there will be a considerable amount of parallel asynchronous processing. The design approach must ensure effective observable control of all processes.

iii) The systems will be in service for about thirty years. It will be necessary to make changes during this period. The systems must therefore be adequately documented to permit effective maintainability.

The above indicate that a highly disciplined approach to the design is required, i.e. a formalised modular design and structured documentation standards are essential. It was decided that the systems should be produced using MASCOT(2) (Modular Approach to Software Construction, Operation and Test) and that the documentation should follow JSP 188(3). These are both UK Ministry of Defence Standards and they are outlined in brief below.

Definition of Mascot

MASCOT is not a programming language nor an operating system, although it includes elements related to both. It brings together a coordinated set of tools for dealing with the design, construction (system building), operation (run time execution) and testing of software. It was developed at Royal Signals and Radar Establishment and is now the method preferred by the UK Ministry of Defence for the design of software in real-time applications.

Aspects of the MASCOT design methodology include:

- Formal method of expressing the structure of real-time software which is independent of computers and programming languages.

- A disciplined approach to design which results in a modular structure, in which functional elements in the design closely correspond with constructional elements at system integration.

- A program acceptance strategy based on the testing of single modules up to larger collections of functionally related modules.

- Simple executive for the control of program execution at run time.

- Flexible method of building systems from individual modules.

- Is applicable at all stages of the software life-cycle, from top level design onwards.

- Provides a basis for management of the software development.

- Compatible with the JSP 188 software documentation standards.

Although MASCOT may be used to design virtually any software system, it is aimed specifically at real-time embedded applications where the software is complex and highly interactive.

Software Modularity. Complex software systems must be decomposed into component parts and functions (modules). Functional decomposition is the sub-division of a system, into a set of parts determined by the purpose of each part, as shown in Figure 4.

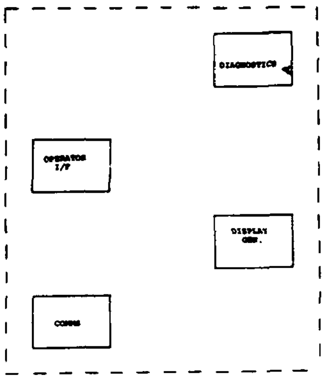


Figure 4 Functional Decomposition

Constructional modularity is concerned with splitting the software into elements which can be separately compiled for subsequent linking and system building (integration), as illustrated in Figure 5.

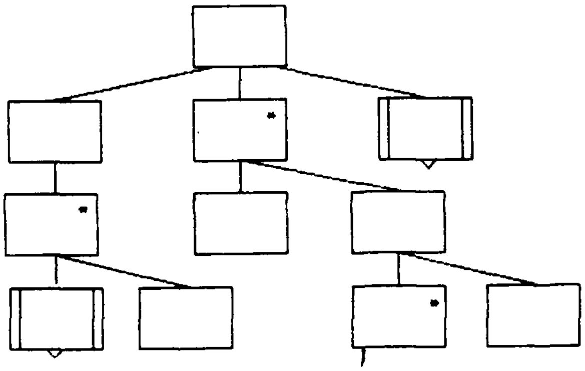


Figure 5 Constructional Modularity

A simple method is required to combine constructional modules to form functional units, otherwise the system building phase becomes too complex. Modules should be defined such that they are fairly independent of one another, with any interaction kept to a minimum. The starting point for the derivation of modularity in MASCOT is the concept of cooperating parallel processes, as illustrated in Figure 6.

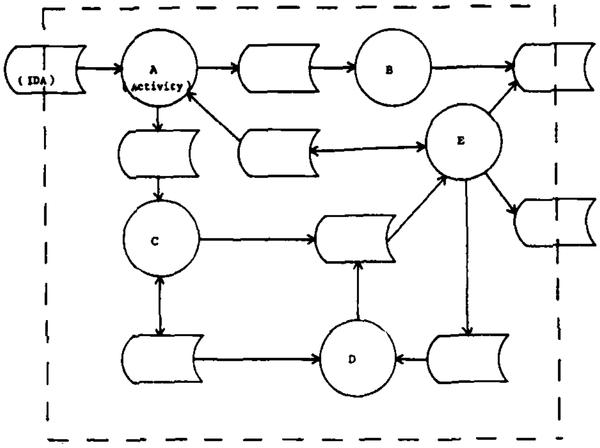


Figure 6 Parallel Processes

MASCOT uses data flow as the main design criteria so a second type of module is introduced - the data areas via which the processes communicate (IDA).

Mascot Software Structure. There are four main elements in the MASCOT software structure. These are:-

i) Activities and IDAs
ii) The ACP diagram
iii) Subsystems
iv) Kernel

i) There are two types of component, or module, in MASCOT - the ACTIVITY and the INTERCOMMUNICATION DATA AREA (IDA). An Activity is a process that conceptually runs simultaneously with all other Activities. It performs a well defined data processing action by reading data from somewhere, carrying out certain operations on that data, and writing a result to somewhere. All input and output of data performed by an Activity must be explicitly defined and controlled.

All data communication between Activities is carried out through IDAs. In general, an Activity will only be connected to a few IDAs.

There are two classes of IDA - the CHANNEL and the POOL shown diagrammatically in Figure 7.

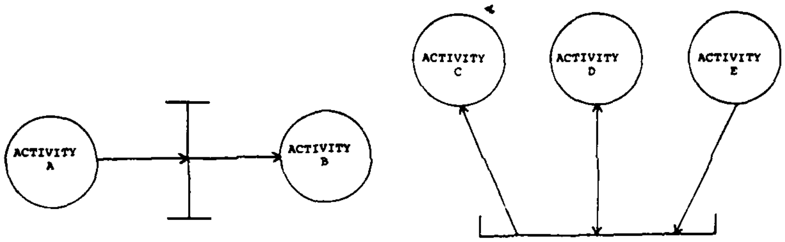


Figure 7 CHANNEL POOL

A channel is used to pass data between Activities and between devices and Activities. It is uni-directional in that data flows one way only.

A Pool is used to hold data for reference purposes - it may be read and updated many times and is not "consumed". Like the Channel, the Pool has an interface via which Activities may gain access to the data within it.

ii) The MASCOT Activity Channel Pool (ACP) diagram defines how the various Activities and IDAs form a software system (or part of a system). A sample ACP diagram is shown at Figure 8.

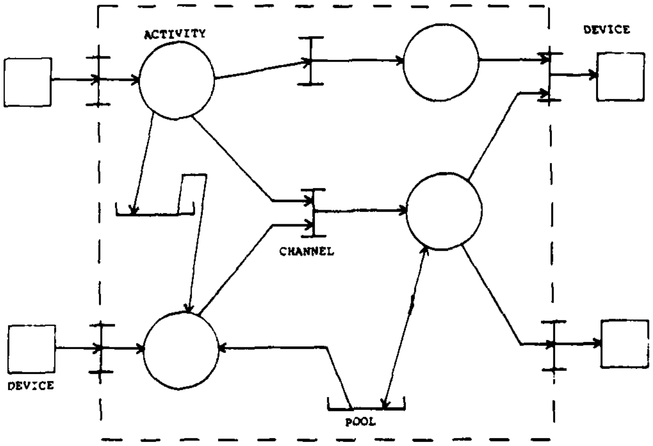


Figure 8 ACP Diagram

It emphasises the message flow concept by showing the data flows between the Activities and IDAs.

The ACP approach is independent of machine, operating system, programming language and application. Another advantage in using it is that the proposed software design is clearly visible.

iii) A SUBSYSTEM is a collection of one or more Activities which perform some recognisable function within the system. The Subsystem is an important MASCOT concept because it is not only a unit of software construction but is also the unit of software that can be controlled within a MASCOT system. The choice of subsystem boundaries is somewhat arbitrary in many cases, although it is usual to split the design in some functional way.

iv) The MASCOT Kernel is a compact real-time executive which provides:

- Scheduling of Activities
- Interrupt handling
- Control of subsystems)
) during testing
- System monitoring)

The interface between Activities and the kernel is by the use of calls which the Activities may execute which are known as PRIMITIVES.

Joint Services Publication (JSP) 188

The documentation standard follows the UK Ministry of Defence standard known as JSP188 (3). This document "introduces common requirements for technical publications to support the 'in service' use, maintenance and subsequent development of the software associated with military operational real-time computer based systems". The standard is formally defined for use as a description of existing systems. We chose to produce our design documentation to follow JSP188 as closely as possible from the beginning of the project. This should result in only minor changes to the documents on completion.

JSP188 calls for a hierarchical documentation system having up to four levels. The standard states that:

> "Only information which contributes to the understanding of the software shall be included in the software publications. Where it is considered necessary for the reader of a software publication to know the functioning of a particular element of hardware or operational procedure, a cross-reference shall be made. to the appropriate hardware or operational procedure documentation; the information shall not be repeated unnecessarily in the software publication.
>
> Generally there shall be four standard levels of documentation, each of the lower levels being a logical derivative of the previous higher level and of sufficient detail to allow an understanding of the software to the detail implicit at that level. Within each level, as many sub-levels shall be created as necessary for an understanding of the system without reference to any of the lower levels. The use of all four, or fewer, levels will depend on the complexity and the requirements of the particular software system."

v) It is a Ministry of Defence standard. There are other design methodologies but as MASCOT is an MoD standard, it is appropriate to use it where it is applicable to ensure commonality across many types of system.

Disadvantages of the MASCOT technique are:

i) It does not readily show the flow of control. This is particularly important for projects such as those under discussion here. This information has to be held separately.

ii) Associated with the MASCOT system are considerable overheads in terms of size and timing. This can lead to expensive processor requirements. Existing systems tend to have to compromise by producing a design which is not pure MASCOT but which follows the spirit of MASCOT. This tends to mean that some of the potential advantages associated with the development of a MASCOT based design are lost. This point is discussed in a later section.

Experience of the top level design of these systems to date has shown us the importance of the statement that JSP188 is a design documentation standard for an existing system. Because we chose to produce drafts at each level in sequence we found that producing the level 1 document immediately after the De Marco requirements specification was not appropriate. The tendency was to put too much detail in the level 1. This meant that a revision was necessary to make it reflect a more appropriate view of the system at that level. The most likely reason for this is that the requirements analysis is very detailed and the tendency was for the level 1 to follow this level of detail, instead of being a functional overview. A design review suggestion was that Level 2 should follow on from the De Marco analysis and Level 1 could then be produced as a top level view. In fact we did subsequently finalise Level 2 before Level 1.

The JSP188 document issues guidelines as to how the system should be described at each level. In some cases these are fairly general. Because we had three different projects with a fourth project producing the common software this lead to difficulties because of slight differences in the interpretation of the standard. We found it necessary, to ensure that consistent documentation results from all projects, to write a statement outlining our approach to meeting JSP188 at each level.

JSP188 can be used to document a MASCOT system provided the interpretation of JSP188 is properly defined. The key point to make is that, as described above, JSP188 gives guidelines as to its use while MASCOT is a formal standard. To combine the two the formalisation of the interpretation of JSP188 is necessary.

A very valuable part of the documentation standard as we use it is that at each level estimates are made of processor loading and memory requirements. This means that problems with certain areas of the system can be identified easily in the design and if possible corrective action can be taken. Our aim at level 2 design was to maintain the processor loading and memory requirements at 50% of that available. Our view is that at this stage of design the loading estimates should not exceed this value.

We have produced documents to follow JSP188 as part of our design. These are live documents in that they will change as the system changes either as a result of new requirements or as a result of errors detected during testing. Maintaining consistency across all the projects under discussion is important because:

a) the implications of errors detected by one project can easily be passed to others;

b) the change of any of the design documents can be achieved more cost effectively.

The combination of the diagrammatic MASCOT descriptions of this modular design coupled with the structured formalism of the JSP188 documentation levels lead to an easily understood and therefore easily maintainable and testable system. This reflects our views on MASCOT and JSP188 which, as UK Ministry of Defence Standards are used on these projects, we would expect that future systems will lead to automatic progression from requirements analysis through computer assisted design.

SOFTWARE DEVELOPMENT

The Phase

The software development phase covers that aspect of the system development from the low level design to the start of system test. At the time of writing most of the projects are nearing the end of the design phase and some have started actual code and test. This section of the paper describes how the software is to be developed, the development environment and the difficulties associated with this part of the programme.

The Development Procedure

The final system is to run with the software in ROM (Read Only Memory) or EPROM (Erasable Programmable Read Only Memory). The development environment must be such that the software can be produced and tested off-line as much as possible. The ROM or EPROM will then be blown, i.e. the software will be stored in memory.

The UK Ministry of Defence have sponsored the development of an environment - i.e. a development facility - suitable for producing software following a MASCOT design. This allows for the formal build, test and control features associated with the MASCOT methodology. This development facility is called CONTEXT and it is used by the projects under discussion.

CONTEXT enables the user to build a software system using the MoD sponsored high level language, CORAL 66. The individual MASCOT modules, i.e the ACTIVITIES, CHANNELS and POOLS are produced and tested separately. They are then linked together and tested as subsystems. The subsystems are then linked together to form a complete system.

CONTEXT is installed on a VAX 11/750 operating under VMS. The programmer can test his software on the VAX itself. This is known as host-target development and enables the programmers to produce software using the full capabilities of the VAX. Once a significant amount of software has been produced or when the testing requires the actual system interfaces then the software must be run on the actual processor itself. CONTEXT copes with this by having a serial link to the remote target which enables the programmer to downline load software to the target and to monitor and debug this software running on the remote target itself. This is illustrated in Figure 9.

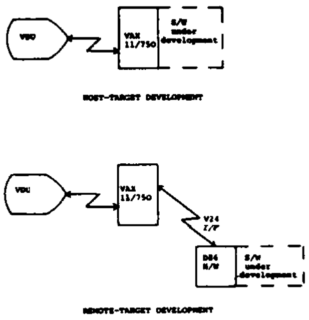


Figure 9 CONTEXT Development

The facilities of CONTEXT include logging of steps through the software, insertion of break points, etc. The CONTEXT log is actually used as a formal test record. The programmer may obtain an assembler language listing off the CORAL programmer under test. The facility also permits the use of actual assembly language modules linked with the CORAL code. This is sometimes necessary for some performance critical software.

During development is is often necessary to work very close to the hardware to check status information, register changes, etc. This is usually solved by using an In-circuit Emulator (ICE). This is a microprocessor development facility which enables one to replace the processor chip with a connector linked via an umbilical to the ICE which has full debug facilities for use at a low level. This is illustrated in Figure 10.

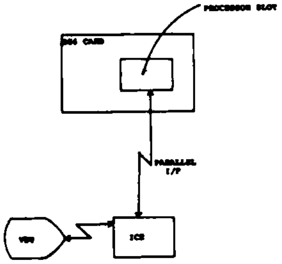


Figure 10 ICE Development

We have used a number of these readily available systems. The logging and control facilities are similar to those offered with CONTEXT but in general they operate at a much lower level.

Problems Encountered

CONTEXT. This facility proved very useful particularly when working with host-target development. However, a number of problems arose because CONTEXT itself has not had a very wide exposure such as a commercial system like DEC RSX-11M would have. This led to a number of delays during development, particularly when working at the machine level, with problems associated with CONTEXT itself rather than the software under development. It would seem that this is always likely to be the case if a not widely exposed development system is used.

During testing if the remote target was lost, i.e. CONTEXT, lost control of the software, then the only way to locate a fault was to use the ICE. This is general is a very slow method of development. Usually these faults occur because of software design or build errors, but in the event of their being related to hardware they are more difficult to solve. This is discussed below.

CONTEXT tends to place a considerable load on the VAX both in terms of ports, i.e. two per target, and in terms of processor loading - not too many users can use CONTEXT at one time.

MASCOT. A standard kernel is held within CONTEXT to permit MASCOT development. Because of its general nature this kernel is not necessarily the most efficient for a given application. It proved necessary to re-write parts of the kernel to enable performance requirements to be met. Certain key very frequently required checks, etc. were actually linked into the kernel itself.

The formal structure of MASCOT tends to lead to considerable processing overheads. This can be overcome by introducing extra processors but usually cost constraints prevent this solution and the software structure is altered slightly to improve performance. This is generally easily achievable with MASCOT but can of course lead to a design which is non-ideal. There will however rarely if ever be a system where compromise to some extent during design is not necessary.

Environment. We refer here to the location of the development teams. The four projects were initially run on three different sites. This was subsequently reduced to two. A number of interesting points are to be noted.

The teams were all producing software with some degree of commonality. It was/is necessary that they should meet regularly to discuss commonality, interfaces, etc. Formal meetings do take place, but of course they are costly in terms of time. However, different site working means that the wealth of exchange which occurs with casual meetings is lost. Our reduction to two sites was to join the applications people together on one site while the other site held those people who produced the firmware, i.e. the common software. This common software is an important part of the project and is discussed in a later section.

SOFTWARE TESTING

When to Test?

Testing is probably the most important part of any software development life cycle. When the software is produced you can't see it; you can't say "It looks all correct". Test must start at the very beginning of design and carry on through to Acceptance Testing.

The Tests to be Conducted

Testing Cycle. There are four main stages of testing which occur chronologically:

i) Module Test
ii) Integration Test
iii) System Test
iv) Acceptance Test

The specification of the tests follows a different route however. At every stage of development the designer defines the next level down from his last level and at the same time he must define the acceptance criteria for testing and how integration will take place. The test plan must be appropriate to the state of the system at that time. A schedule for tests at a particular level cannot be done if the design for that level has not been done, but has to be done before the design gets so detailed that it can no longer be covered adequately. The stages that are employed in the development cycle for the four projects under discussion are shown in Table 5.1 with the associated test plans listed as they will occur. The test list doesn't include design reviews which are held at significant milestones during development and form part of the overall test strategy of any system.

Test Plans. The Acceptance Test plan states the philosophy to be adopted in accepting the system to be produced. The System Test plan states the philosophy to be adopted to completely test all aspects of the system to be produced. In the most highly reliable systems both Acceptance and Systems tests will be identical. The detailed schedules for these tasks often cannot be produced until later in the development phase around the time of the start of Integration test.

The Integration Test plan describes how the modules or subsystems defined during the level 2 design phase will be linked together to build a total system. The modules test plans themselves are produced immediately post level 3 design and prior to the start of level 4 - the code and unit test phase of development.

The reason why test plans are produced in this way is that the designer is forced to think during the design phase how his system is going to be tested. This, done properly, is sure to result in a good unambiguous well-conditioned design. It will be good because to define the test he must review his design. He may find faults which can then be corrected. These may be faults of omission or ambiguity - you can't specify the test if the design is unclear. The design will be better conditioned because part of defining the tests is to include all paths of execution. Defining all these paths may show an ill-conditioned response inherent in the design.

Development Tests. The Module tests are conducted to ensure the correctness of each software module in isolation. Formal test records must be maintained at this and subsequent levels of testing.

Integration Tests link the modules together to form subsystems. The culmination of Integration testing results in a complete system. It is during this phase of testing that the best opportunity for eliminating design errors arises. For small systems we often follow the route of top down design and bottom up build. For larger systems we often do bottom testing of modules but integrate from the top down. For very large systems very often horizontal build is more appropriate. This results in a build where recognisable complete elements of the system are testing as early as possible during integration. It is always important to test the difficult parts of a system as early as possible but at the same time trying to maintain some overview of the system.

System Testing enables the final resolution of interface problems which arise when running the complete system. It is also the first real opportunity to check on actual system performance and suitability. It is usually the most frenetic part of the life cycle! Typically the time spent on integration and system testing can amount to 30% of the total development time.

Acceptance Tests are usually a subset of the System Tests and constitute the formal final testing of the system. They usually accompany a series of informal tests by potential users to give the system as much exposure as possible in the early stages.

PROJECT PHASE		TEST DOCUMENT
Requirement Analysis	——————>	Acceptance Test Plan System Test Plan
JSP 188 Level 1		
JSP 188 Level 2	——————>	Integration Test Plan
JSP 188 Level 3	——————>	Unit Test Plan
JSP 188 Level 4		
Integration Test		
System Test		
Acceptance Test		

Table 1 - System Development

Problems with Testing

One of the main advantages of MASCOT is that it is a design technique which does specifically take account of testing. This means that testing by linking MASCOT modules into subsystems and then system building is made more easy. The main effect of MASCOT is that the concept of isolated data areas and very rigorously specified interfaces reduce significantly the errors which normally arise during testing.

Many problems usually arise in testing the hardware software interfaces. These have been largely overcome by having all such software developed by the firmware team who are ahead of the application teams. These interface problems will thus have been solved before the start of integration testing by the application teams.

SYSTEM RELIABILITY CONSIDERATIONS

Software Correctness

Many people new to software often ask the question "how reliable is it?" The term is inappropriate to software because software is 100% reliable. It is correct or incorrect. The aim in software design is to ensure that the software to be produced will be correct and will remain so even in the event of change. To achieve this one must have adequate Quality Assurance procedures to be applied during system development, appropriate mechanisms for configuration control throughout the system life and if possible use software which has already had some exposure. These important factors are discussed below. It is apparent that only by rigidly applied discipline can any "reliability" be guaranteed.

Quality Assurance

There is no method for proving the correctness of a software module. Confidence can only be built up if a demonstrable acceptance set of standards have been applied at all stages of design development and test. We produce a Project Plan at the start of a new project which says what we are going to do. It is most important that a Quality Plan is also produced which says how we are going to do it. For related projects such as those under discussion here, one expects the QA plans to be similar and indeed this is the case. The design standards have been described above. During development it is vitally important that adequate test records are maintained. Many systems experience difficulties because during development testing at each stage has not been conducted properly. Design Reviews validate the design. Technical QA reviews ensure that the rules laid down as being appropriate for a given project are adhered to. This discipline of formal quality must pervade the project and be clearly visible to the external viewer. Sometimes software systems are not accepted because although they may be correct no clear quality procedures have been followed. Observable quality is thus one of the keys to a successful software project.

Configuration Control/Maintainability

The concept of rigid change control procedures and methods for deciding which drawing modifications have long been standard for hardware systems. Not many automated schemes exist for software. On these projects we make use of a recently developed computer based software configuration control system known as LIFESPAN. This is currently under evaluation for the Ministry of Defence to determine its suitability for use on MoD projects. It ensures uniqueness of all the software modules and can indicate how changes in one area can affect another.

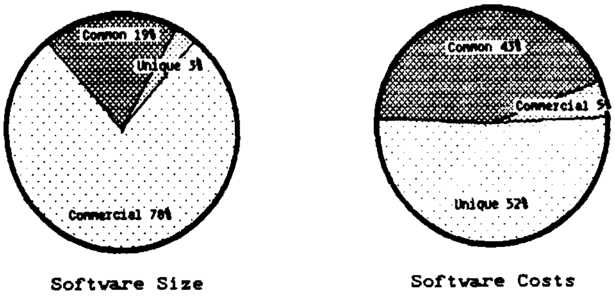
Configuration control should start at the beginning of coding and must be rigidly adhered to. There is always the temptation at system test to effect "quick" changes in the form of patches to the code. These tend to be forgotten about and can result in a system which cannot be rebuilt. The projects under discussion should overcome this problem by using LIFESPAN which will be managed by someone not on the project team. Formal discipline will thus be applied from the outset. This will continue to be the case throughout the life of the software which may be up to 30 years.

Software Exposure

One method of enhancing overall system reliability is to use as far as possible software which has had some exposure. For the project under review many elements of the software are common. These subsystems were produced early in the development cycle and run as frequently as possible to eliminate any errors. These subsystems include:

i) Communications
ii) Input/Output Handling
iii) Diagnostics
iv) Man Machine Interface
v) Maintair.er Facilities
vi) Displays

These elements are key to the total system and by ensuring commonality as far as possible the likelihood of errors remaining post test should be considerably diminished. The production of the overall software system is also more cost effective. The cost of unique software is shown in Figure 11.



Software Size

Software Costs

Figure 11 Software Size and Cost Percentages

The more software is exposed the more likely it is that it will be correct. This quantitative statement may be true but does not inspire much confidence. A more useful indication analogous to the MTBF parameter for hardware is the parameter Time to Next Fault detected. It has been suggested (4) that by logging the faults detected during development and classifying them in terms of project phase, i.e. concept, specification design, etc., it is possible to predict when the next fault will occur. We have some experience of applying the Duane technique to previous projects with some indication of success. A similar log of faults detected during development will be maintained for these projects and we hope that this will enable us to make predictions relating to system reliability.

A PRACTICAL PROBLEM

The above sections discuss the techniques we have employed in meeting the RN requirements. In this section we discuss the practical problems associated with producing the software to control a hypothetical ship propulsion system as shown in Figure 12.

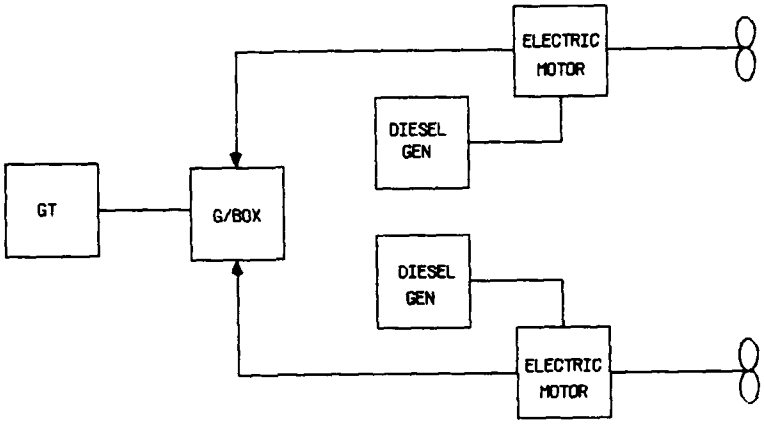


Figure 12 Propulsion System

The configuration illustrated may be a first look as opposed to the final configuration. Our first task is to produce a requirements analysis for the control of this plant. It is likely that our first attempt will show that we haven't defined many of the interface requirements, particularly in relation to the control of auxiliaries. The iterative process of completing the De Marco analysis will involve both the systems engineers responsible for the plant and the software engineer. Working closely together they can discuss the practical problems associated with controlling the plant effectively and as is often the case, the systems engineer may feel the need to change his requirement as a result of considering how plant control can be effected. He may wish to use more than one Gas Turbine because of the problems associated with one. All these changes can readily be made to the De Marco document. It is important to point out that at this stage we should not have to consider hardware or software, but just the requirement. Sometimes this is impractical as the hardware may already have been selected. This poses a severe limitation on which requirements can be met and on how the control system can be designed.

Given a firm requirement a design can be produced. The facilities for this system (in JSP 188 terms) could be:

i) Control
ii) Primary Surveillance
iii) Secondary Surveillance.

The Mascot subsystems would include:

i) Input/Output
ii) Man Machine Interface
iii) Interprocessor communications

iv) Surveillance
v) Control
vi) Maintenance and diagnostics.

The system configuration could be as in Figure 13

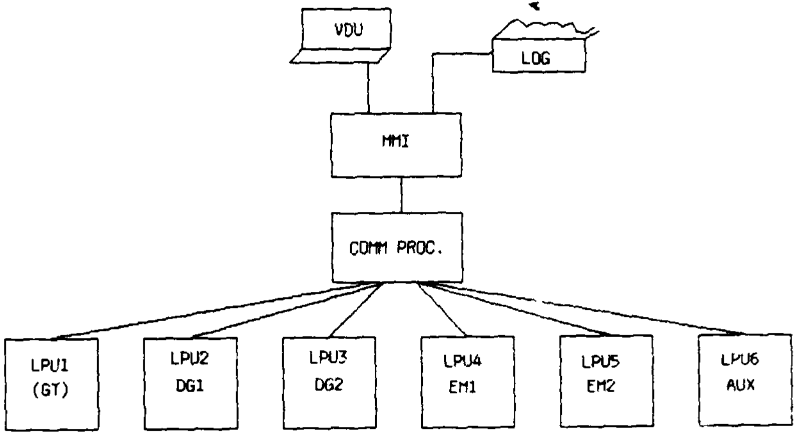


Figure 13 System Configuration

with one Local Processor Unit (LPU) per plant element. Design considerations must take account of system performance and reliability reouirements explicitly.

The configuration shown displays a star network. This is reliable in that the failure of a link to an individual LPU does not cause the total system to fail as the other LPU links can still function. A ring network could sustain one failure provided extra software was written to effect polling in both directions from the communications processors. However if the links to LPU1 and LPU6 fail in a ring network as shown in Figure 14,

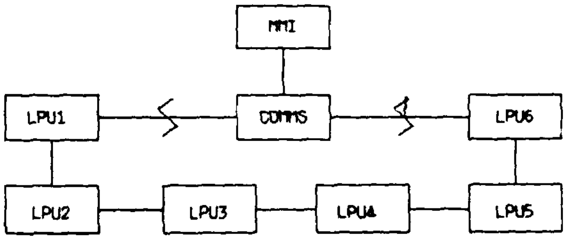


Figure 14 Ring Network

then the whole system can fail. The star network places a considerable load on the communications processor which must be allowed for. Reliability requirements may require that two communications processors be employed. The above are all considered early during the design to ensure that the requirements are met. Processor loadings are estimated at each stage of design and this may indicate a requirement for an extra processor, e.g. two auxiliary processors may be required. Too often the designer says "there isn't enough data/information to do loading/memory estimates now. I'll do it later". This is acceptable in a world of unlimited hardware but we know that is never the case. Proper discipline during design is essential.

During the design phase it is inevitable that changes will come through which are outside the control of the team. It is most important that these are documented correctly to ensure that all levels of design documentation are consistent. This can only effectively be achieved in a top down fashion, i.e. change the requirements document first and then each level of design as appropriate. It is only by applying proper discipline at this stage that we can ensure an effective system will result.

The testing of the system is also achieved in a structured way. The units of software are tested individually, building up to completing the modules for each LPU. This can often be achieved by using one LPU reconfigured to look like each of LPU1 - LPU6 in turn. This is usually more practical because of hardware production schedules. Once all LPUs have been tested individually they are integrated to form the complete system. It is essential to test the total system off-line before presenting it to the ship plant. We know from experience that faults will still exist at this stage of development. A simulation of the elements of ship plant to be controlled must be produced. Using this simulation model of the ship's plant the control system can be tested through all its sequences including those close to the limit of its ranges. When the above tests have been completed the control system can be tested on "real plan". Because of interaction between one system and another and because, practically, no simulation is perfect it is best to test the control system on real plant in a test environment, not on the ship. This requires extensive test facilities but enables final testing to be conducted in a far more benign and practical test environment than the machinery space on a vessel.

The system will then be installed on a vessel and go through sea trials and acceptance. Changes will be required and it is at this time that the value of producing a well documented structured system becomes apparent. Early systems on ship in the weapons area have been extremely expensive to maintain because of the lack of appropriate standards.

THE PAYOFF

The use of digital techniques for control of ship plant can result in significant saving on UPC and permits easier modification later. This is true of all but simple systems. It is valid to state that the development costs are greater because the cost of software development is high. A key point to make however is that through life cost is lower not just because the UPC is less but because system reliability is enhanced. As stated earlier in the paper, software is 100% reliable - once it has had all bugs removed. Exposure of the software in as wide a field as possible results in the elimination of any errors which may remain post-test. Thus overall system reliability can increase with time. Experience of systems in areas outside the sphere of ship plant control has shown this to be the case, e.g. industrial plant control systems effecting plant automation.

FUTURE ROLE OF SOFTWARE IN SHIP CONTROL SYSTEMS

In recent years we have seen the advent of the use of sophisticated man machine interface software in nearly all computer systems from the personal computer to the most advanced management information tools.

Controlling ship plant is however somewhat different to checking our bank account and pointing out the errors. The reliability and availability requirements for ship plant control, particularly in the case of submarines, are very stringent. There exists considerable doubt as to the reliability of systems using digital methods where analogue methods have been used in the past. Recent development in techniques for design and production of software have served to increase confidence in system correctness. In future years we will be better able to predict the likely time to the next failure of the software using data derived from existing systems and predictive models which exist now. Reliability of hardware systems is enhanced today by the use of hot-standby systems. Current research into the development of fault tolerant software indicates that the same principles can be applied to software. There is thus every indication that demonstrable proof of software correctness can be obtained by using techniques somewhat similar to those employed for hardware.

Sophisticated software will become part of future control systems for ship. We are today starting to use full digitised control of ship plant but we still maintain the use of outmoded displays in the form of very expensive mimic diagrams and analogue meters. Apart from the expense of these items they occupy a considerable amount of space in the machinery control room and are very difficult to modify. Smaller colour VDUs showing reconfigurable displays which include user configurable schematics tables, etc. will offer a more cost-effective solution. Features such as machinery condition monitoring will be added, employing extensive analytic techniques implemented in software. Thus the overall percentage of software in future systems is likely to increase. The young people today who will run our systems of tomorrow have considerable exposure to sophisticated computing machines. They will expect the systems they work to be similarly developed.

CONCLUSIONS

We have presented our approach to the production of machinery control and surveillance systems using digital techniques. We have concentrated on those aspects that effect overall system effectiveness, reliability and maintainability.

Software is a new discipline to many people, particularly in the area under consideration. It is vitally important that awareness should be developed relating to the discipline required to produce software that is demonstrably correct and is easily maintainable. Too many systems exist which are claimed to work but proof is not easily available and maintenance by anyone other than the developer is almost impossible. We believe the techniques outlined here are the minimum required to produce a reliable, maintainable system.

There are many systems which employ software for surveillance and simple displays. Some systems effect digital control and many more are under development. Future systems will include more sophisticated man machine interaction capability and extra features such as machinery condition monitoring. Thus future systems are likely to have a far higher proportion of software to existing systems.

The higher proportion of software will lead to more cost effective, reliable and flexible systems than have been available hitherto. This will, however, only be the case if proper standards are employed at all stages of the development from the specification of the requirement through testing and system maintenance for the life of the equipment. Software systems do achieve high reliability and such systems can be applied to produce the best Ship Machinery Control and Surveillance systems of the future given the correct disciplined approach.

REFERENCES

1. Structured Analysis and System Specification
   T. De Marco, Yourdon.

2. The Official Handbook of MASCOT
   Joint IECCA and MUF Committee on MASCOT (JIMCOM).

3. Joint Services Publication 188 (JSP188)
   3rd edition, March 1980.

4. Software Engineering Economics
   B. W. Boehm, TRW.

MICROPROCESSOR BASED PROPELLER PITCH INDICATING SYSTEM FOR A DDH 280

by R.K. Santo
P.V. Penny
Department of National Defence(CANADA)

ABSTRACT

There is a requirement, particularly in warships, to be able to determine propeller pitch to a resolution of at least 0.1 degrees. The essential reason for this is the known improvement in ship's noise signature, which, for warships engaged in anti-submarine warfare, is of critical importance. Various methods are available for measuring propeller pitch. This paper will concentrate on the shortcomings of the existing system in the DDH 280 Class and a unique replacement. The replacement system approaches the required resolution, is repeatable and could be produced at reasonable cost.

INTRODUCTION

The DDH 280 Class of ships is driven by a COGOG (Combined Gas or Gas) propulsion plant in conjunction with two controllable pitch propellers. Ship's speed is ordered by a telegraph knots setting and then automatically maintained by a pneumatic propulsion control system which holds both the propeller shaft speed and the propeller pitch to their scheduled values for the ordered ship's speed. At low manoeuvring speeds, the ship's speed is controlled by varying the propeller pitch with the shaft speed held constant. Higher ship's speeds require the propeller pitch to be held constant, at an upper limit, while the propeller shaft speed is controlled to produce the ordered ship's speed. A typical propeller pitch/shaft rpm profile is shown in Figure 1.

Close control of propeller pitch is important, as variations of one degree of propeller pitch can cause changes of as much as ten percent in propeller shaft power and torque, depending upon propeller shaft speed. For example, at high speeds a change in propeller pitch of one degree can produce a perturbation of several thousand shaft horsepower[1]. At somewhat slower speeds, it has been implied that overall propeller pitch control to better than one degree would not be an unreasonable method of reducing underwater radiated noise orginating from shaft power imbalances[2]. Clearly, this would suggest that a feedback device accuracy of at least one tenth of a degree would be a desirable goal.

The key to proper control of propeller pitch is dependent on the ability to make accurate measurement of the actual pitch on the propellers. Indication of actual propeller pitch in the DDH 280 Class ships is required for the pneumatic propulsion control system and for the information and alarm systems. Unfortunately, the type of pitch indication feedback device currently installed in the DDH 280 Class is

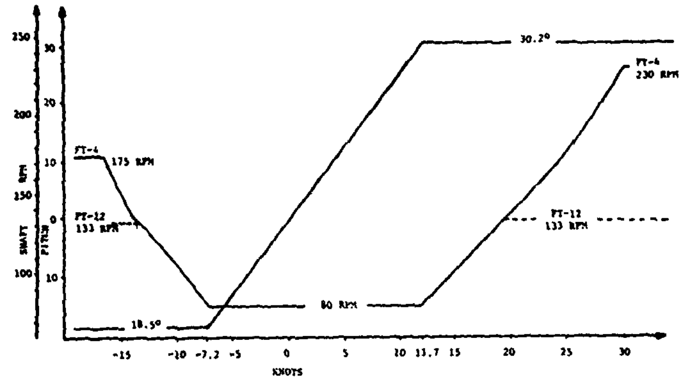
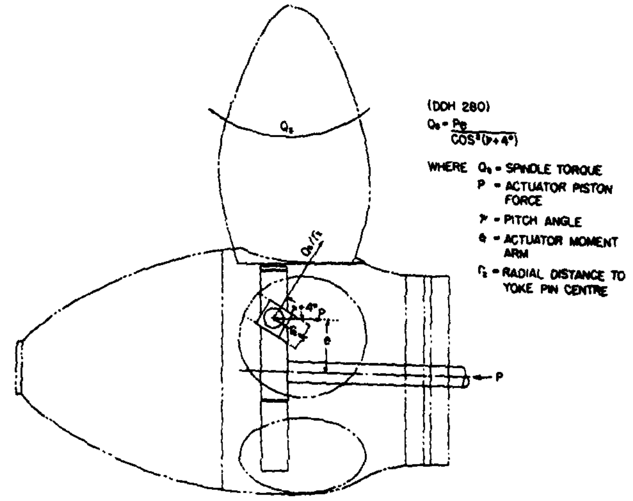


Figure 1. Typical pitch/rpm profile



Q_s
Q_s/r_2
$\gamma+4°$
P
e
P
(DOH 280)
$Q_s = \frac{Pe}{\cos^2(\gamma+4°)}$
WHERE Q_s = SPINDLE TORQUE
P = ACTUATOR PISTON FORCE
γ = PITCH ANGLE
e = ACTUATOR MOMENT ARM
r_2 = RADIAL DISTANCE TO YOKE PIN CENTRE

Figure 2. Propeller Hub Mechanism

the weak link in the overall propeller control system. Clearly, any provements to the feedback device that would resul' in a better indication of propeller pitch would have numerous beneficial side effects. With the advent of more sophisticated digital machinery control systems, such as the Canadian Navy's Shipboard Integrated Machinery Control System (SHINMACS)[3] with it's ability to cater for various control strategies, improvements to the feedback device become even more attractive.

Propeller Pitch Actuation

The propeller pitch actuation mechanism in DDH 280 Class ships includes a push-pull rod which drives a yoke in the propeller hub as shown in Figure 2. The yoke is used to position the blade via a radially sliding block in the blade foot. Deformation of the push-pull drive rod under load requires a sensing rod to be installed to give proper indication of the actual pitch position.

With one end of the sensing rod connected in the propeller hub, the position of the inboard end of the this rod is indicated by the longitudinal motion of a feedback ring on the exterior circumference of the propeller shaft. This arrangement is shown in Figure 3. The position of the feedback ring is referenced to a static ring which does not move relative to the shaft.

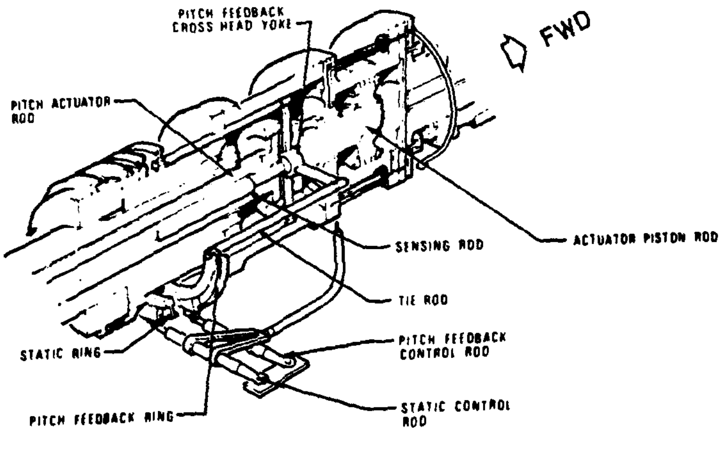


Figure 3. Feedback Ring Arrangement

The displacement between the two rings is therefore directly related to propeller pitch, but because of the blade foot sliding block arrangement, the input/output relationship is non-linear. The relationship is defined by the following equation:

$$Y = 4.0 - \text{ArcTan}\ \frac{(X-X_0) + (0.5506)}{(7.874)}$$

where: Y = the propeller pitch in degrees measured at 70% of the radius;
X = the ring displacement in inches; and
X_0 = a constant equa. to the ring displacement in inches when the propeller pitch is zero.

EXISTING INDICATING DEVICES

There are currently two pitch indicating devices installed in DDH 280 Class Ships, both of which use a common set of connecting arms to sense the displacement between pitch feedback rings. The connecting arms track the position of the rings through two sets of phenolic shoes that slide on the machined surfaces of the rings. Experience has shown that wear of the phenolic shoes can produce large errors in pitch indication and any eccentricity that may occur between the two rings will cause fluctuations in the pitch readout. Also there is considerable mechanical signal loss due to the indicating devices being mechanically connected near the fulcrum of the connecting arms. This arrangement is necessary to ensure that the devices are clear of the rotating shaft and to minimize the connecting arm displacement.

The first of the two existing indicating devices produces a pneumatic output signal proportional to propeller pitch. The mechanical signal from the connecting arms is conditioned by the use of a shaped cam which compensates for the trigonometric relationship between the rings and the propeller pitch. A pneumatic output is produced after this compensation to provide the feedback signal required by the pneumatic propulsion control system.

The second installed indicating device produces an analogue electrical output signal. In this device, the mechanical signal from the connecting arms is conditioned by several mechanical linkages which again compensate for the aforementioned trigonometric relationship. Subsequent to this signal conditioning, an electrical output is produced through the use of a Linear Variable Differential Transformer (LVDT). The electrical output provides propeller pitch position information to several alarm and information systems.

The electrical feedback device was installed subsequent to the installation of the pneumatic device in an attempt to improve the accuracy of the feedback signal, and although the electrical feedback device does indeed have slightly better accuracy than the pneumatic device, problems such as misplaced design documents and obsolete components have contributed to calibration and maintenance difficulties. As a result, both devices have remained in use; one for the pneumatic propulsion control system and one for the electrical information and alarm systems.

It is interesting to note that the deceptively simple trigonometric relationship between the pitch feedback rings and the actual propeller pitch has often caused confusion for technical personnel involved in adjusting and calibrating the pitch indicating devices onboard the ships. In most sensing devices, a zero adjustment at the input would generally result in the correct offset at the output, as the input and output are normally directly proportional. However, because of the trigonometric input/output conditioning required for this specific application, an adjustment at the input results in a nonlinear bias in the output. The net effect of this adjustment is an erroneous pitch indication. The magnitude of this problem was further demonstrated when it was discovered that the engineering firm, who had done so well with the development of the new propeller pitch indicating device, and who had considerable technical appreciation of the system, allowed the same misconception to creep into the instruction manual. Needless to say it has taken considerable effort to overcome this confusion.

FEASIBILITY STUDY

A feasibilty study was initiated to determine the possibility of developing a more reliable, accurate and repeatable type of pitch indicating device. As this device was to be used for a retrofit, certain suggestions, such as mounting a sensor directly in the propeller hub, were left for applications involving new construction.

Although hub mounted sensors were not considered in this development it is felt that for new propeller designs it is highly desirable that propeller-mounted sensors be considered as an integral part of the initial propeller design process rather than as a separate design effort. State-of-the-art sensors far surpass the capabilities of potentiometric type sensors that were used a few years ago. Hence, if control system and propeller designers were to work together rather than in isolation, a reliable, repeatable and accurate propeller pitch indicating system could evolve. For example, with the proliferation of relatively inexpensive sensors, redundant sensors could be installed to increase system availability and as the mechanical/electrical interface moves closer to the propeller, the total system indicating accuracy should improve noticeably.

Regardless of the optimum sensor position, mounting the sensing device directly on the (inboard) propeller shaft did offer attractive advantages for this development project. A requirement for an indicating instrument accuracy of ±0.1 degrees was chosen as a realistic goal which resulted in a requirement to read ring position to approximately ten thousandth of an inch. This accuracy is sufficient to avoid significantly degrading the overall control system accuracy. It should be noted, however, that it was not intended that actual pitch would be read to this accuracy, only the position of the pitch feedback rings. Problems such as temperature changes in the shaft and the accompanying contraction and expansion, wear and clearances in the blade linkages, etc., could effect the overall accuracy of the indicated pitch by more than plus or minus three quarters of a degree over and above the indicating device accuracy[2].

An LVDT was chosen as the sensing device because of its inherent ruggedness and its capability to make precise, repeatable, displacement measurements over a relatively wide range. LVDT's also remain relatively stable when subjected to environmental temperature changes.

United States Coast Guard experience had indicated the superiority of telemetry systems over slip ring devices for removing information from rotating shafts in similar applications. The availability of a commercial telemetry device similar to one that is already in use in Canadian Naval ships made this the obvious choice. Although expensive, the use of a proven telemetry device was more desirable than developing a new telemetry unit and no doubt increasing the overall risk of the project. The new propeller pitch indicating device may be modified at a later date to incorporate less expensive telemetry circuitry as a result of ongoing design efforts.

Several options were available for obtaining the necessary trigonometric signal conditioning, such as analogue circuits, microprocessor controlled mathematical packages, and digital look-up tables. To meet the requirements of low cost, fast response with high precision, and especially flexibility, the digital look-up table method using eraseable-programmable-read-only-memory (EPROM) was chosen.

Table 1. Test Results

Position (inches)	Theoretical (volts)	Actual (volts)	Difference (volts) (Theor. - Actual)
-4.75	4.01	4.00	.01
-4.50	3.83	3.83	.00
-4.25	3.65	3.66	-.01
-4.00	3.46	3.46	.00
-3.75	3.26	3.27	-.01
-3.50	3.07	3.08	-.01
-3.25	2.87	2.88	-.01
-3.00	2.66	2.67	-.01
-2.75	2.45	2.46	-.01
-2.50	2.24	2.24	.00
-2.25	2.02	2.03	-.01
-2.00	1.80	1.82	-.02
-1.75	1.58	1.61	-.03
-1.50	1.36	1.38	-.02
-1.25	1.13	1.15	-.02
-1.00	0.91	0.91	.00
-0.75	0.68	0.69	-.01
-0.50	0.45	0.46	-.01
-0.25	0.23	0.22	.01
0.00	0.00	0.01	-.01
0.25	-0.23	-0.22	-.01
0.50	-0.45	-0.44	-.01
0.75	-0.67	-0.66	-.01
1.00	-0.89	-0.86	-.03
1.25	-1.11	-1.10	-.01
1.50	-1.32	-1.31	-.01
1.75	-1.54	-1.50	-.04
2.00	-1.74	-1.73	-.01
2.25	-1.95	-1.92	-.03
2.50	-2.15	-2.11	-.04
2.75	-2.34	-2.31	-.03

DEVELOPMENT

As many of the design considerations were researched during the feasibility study the follow-on development work went quite smoothly. Development of circuitry to interface the LVDT to the electronics for the shaft-mounted telemetry system involved commonplace components. Also, the microprocessor circuitry for the look-up tables used a familiar technology, so neither task presented much difficulty. The use of microprocessor based device enabled the design to easily cater for corrections as a result of ambient temperature changes. As was mentioned previously, the choice of a commercial telemetry unit kept the risk in this portion of the system to a minimum.

As can be seen from Table 1, which is taken from the latest test report [4], the new propeller pitch indicating device was linear to within approximately ± 0.2 degrees and accurate to approximately ± 0.3 degrees. It should be noted that in Table 1, 125 millivolts is equal to 0.100 degrees of pitch. Actual engineering trials in HMCS Huron indicated that the device worked as effectively at sea as it had on the laboratory test jig. Pitch indication readouts versus ring displacement measurements were taken with the propeller shaft stationary and subsequent observations were then made at sea under dynamic conditions. The device will undergo further testing at sea in the fall of 1984 when it will replace the existing sensing devices in a fully operational test lasting several months.

NEW PROPELLER PITCH INDICATING DEVICE OVERVIEW

The pitch on the propeller is, of course, the parameter that is intended to be measured. As no two propellers are manufactured precisely the same, measuring the rotation at the blade foot will in fact introduce some small amount of error but in a practical sense this cannot be avoided. The new propeller pitch indicating device is best understood by reviewing the signal path block diagram shown in Figure 4.

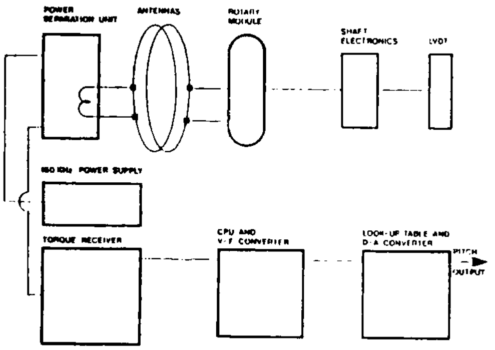


Figure 4. Signal Path Block Diagram

The propeller pitch mechanical signal is directed back via the sensing rod to the pitch feedback rings where the propeller pitch can be extracted as a trigonometric function of the displacement between these rings with the associated minor linkage inaccuracies as was explained previously.

At this point, the mechanical signal is converted to an electrical signal through the use of an LVDT which is mounted on the propeller shaft with the appropriate custom manufactured LVDT core and body mounting brackets. The LVDT must be centred to give zero output at a predefined ring displacement which is normally the midpoint of the propeller pitch actuator range and not necessarily at zero degrees of pitch. The LVDT supplies a bipolar DC output voltage that is proportional to the pitch feedback ring displacement about this centre point.

The analogue electrical signal is then conditioned by a resistor network to make it acceptable to the input of the telemetry system. Included with this shaft-mounted circuitry is a second circuit which is used to supply the LVDT with its required stable input voltage. The raw supply voltage is obtained from the telemetry system which is capable of supplying power to the shaft-mounted components via a radio frequency signal as well as removing signal information in the reverse direction.

A rotary module fastened in the rotating collar accepts the signal from the resistor network and transmits it as a frequency modulated signal to the stationary loop. The power separation unit separates the incoming analogue signal from the outgoing power supply signal and then sends the analogue signal to the display unit for further amplification. At this point, any slight misalignment of the LVDT position on the shaft can be compensated for with electrical zero and range adjustments.

Some minor circuitry is included to ensure that the analogue signal is correctly prepared for the voltage to frequency converter which follows. Additional electronic adjustment is available to obtain the correct LVDT centre position. An integrated circuit transforms the propeller pitch analogue voltage signal to a proportional frequency signal.

At this point in the signal path the analogue signal is converted to a digital signal. A single-board computer controls a pulse counter over consecutive ten-millisecond periods and uses the count of the frequency converter output as the address for the look-up table. The look-up table uses 4096 address locations to store the information required to relate the pitch feedback ring displacement to the actual propeller pitch. Data from the look-up table, at the appropriate address, is transmitted to a buffer circuit and then passed on to the digital to analogue converter. Zero and full scale adjustments are available in the digital to analogue converter circuitry to calibrate the propeller pitch output signal.

An operational amplifier is included to supply sufficient signal strength for the ship's systems and an integral digital voltmeter is available with the correct scaling to provide a local readout of degrees of propeller pitch. It is highly likely that this final analogue portion of the system will be removed at a later to date so that it may interface directly with the replacement machinery control system to be fitted in the DDH 280's.

A picture of the hardware, without the protective enclosure and stationary antenna mounting hardware, is shown in Figure 5.

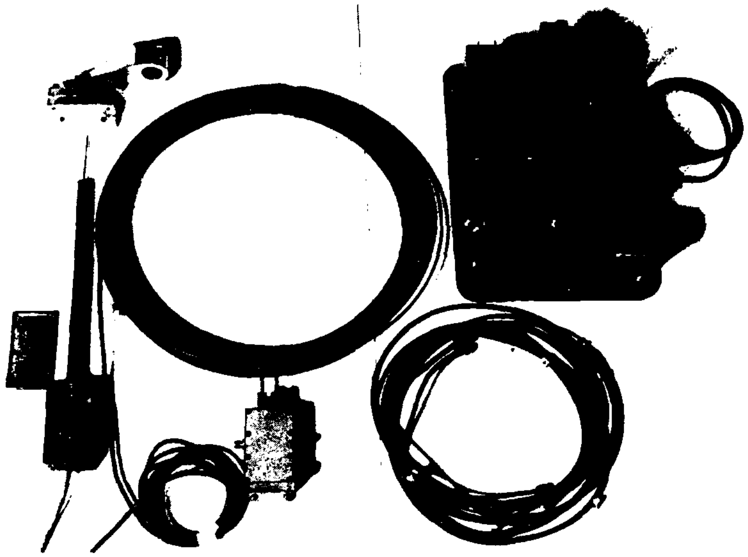


Figure 5. System Hardwaree

CONCLUSIONS

For warships, particularily those engaged in anti-submarine warfare, there is a requirement to minimize emitted noise. It is well known that the properties of variable pitch propellers can be used to advantage for improving the ship's noise signature in the sense of minimizing emitted noise. To control the propeller pitch within the required accuracy there is a need to have a feedback device that gives a precise indication of propeller pitch.

Although the design goal accuracy of ± 0.1 degrees was not quite met, the development project has produced a device with improved performance characteristics. hence in this sense the development is considered a success. There were many new ideas generated from this development that could significantly enhance the current product. These ideas will be pursued if the results of the upcoming sea trials are positive.

The sensing device should be installed as close to the propeller blades as practical so as to minimize inherent system errors. As the optimum design location of the sensing device is dependent to a great extent on the state of sensor technology, it should be easier to meet this requirement for future pitch indicating sensors.

As digital sensors become more common, the interface between the analogue (real world) signal and the digitized (control system) signal can also be moved closer to the propeller blades. Also, as modern propulsion control systems almost invariably require digital input signals, the sooner the conversion is made in the signal path, the better the feedback signal accuracy will be.

REFERENCES

(1) B.D. MacIsaac and R.J. Dupuis, "Final Report DDH 280 New Design Propeller/Propulsion Control System Computer Simulation", GasTOPS Ltd. Reference GTL-TR-7-15.3, March 19, 1984.

(2) LCdr R.W. Allen(RN) and I.E.F. Ogilvie, "Control Requirements for Future CPPs", Sixth Ship Control Systems Symposium Vol. 4, Ottawa 1981, pg. P 2-1.

(3) Cdr B.H. Baxter, LCdr R.J. Rhodenizer and P.V. Penny, "Shipboard Integrated Machinery Control System (SHINMACS) - A Canadian Forces Concept", Sixth Ship Control Systems Symposium Vol. 5, Ottawa 1981, pg. M 2-1.

(4) Davis Engineering Limited, Ottawa; "Improvements to the Propeller Pitch Indicating Device": Reference 82-128.3, June 1983.

Acknowledgements

The authors would like to thank S. Lamirande and J. Watson for their efforts in producing the figures and collating test data.

DESIGN OF A MAN-MACHINE INTERFACE FOR SUPERVISORY AND MANUAL CONTROL OF SHIP SYSTEMS

by J. Vermeulen
Institute for Perception TNO
Soesterberg, The Netherlands

ABSTRACT

During the last decades control of ship systems has been changed from local, manual control to remote control from a Technical Control Centre (TCC). Initiated by both the tendency to reduce ship complements and the progress in technological development, more and more ship systems are controlled by Automatic Control Modules (ACM). As a result the operator task has evolved from an active manual control task to a more passive supervisory task.

On the Walrus-class submarines of the Royal Netherlands Navy, now under construction, many systems will be controlled by ACM's. In the TCC the central part of the two workplaces are formed by two VDU's that are used for the presentation of error messages, system state information, trend diagrams, etc., and for interactive manual control of ship systems under some circumstances. As a result the man-machine interface and the operator task will differ very much from those on the present Zwaardvis-class submarines.

In this paper the design process of the operator panels and the process schemes on the VDU's will be described from an ergonomic point of view. The console design is tested in a static simulation experiment in a scale 1:1 mock-up. The design of the process schemes is tested in a dynamic simulation experiment on a colour VDU.

INTRODUCTION

In control and supervision of technical systems on new ships for the Royal Netherlands Navy (RNN) computers and VDU's will play an important role; in future this role may even increase in importance. The present situation is the end of a twenty-year development in which level of automation has increased and ship's complement has decreased.

This development started about two decades ago when the RNN decided that new ships should sail with an unmanned machinery room and a significantly reduced crew. That decision had been the result of the navy staff requirements to reduce running costs in both the personnel and the material field. Technological progress made it possible to realise a higher level of automation and a reduced crew in a responsible way. This resulted in a series of frigates (Tromp- and Kortenaer-class) on which the technical systems are monitored and partly controlled from one central room. From this room, the Technical Control Centre (TCC), the ship's safety control system is monitored as well. The lay-out consists of a row of panels with alarm indicators and controls, and a row of consoles with mainly communication apparatus. The alarm indicators consist of lamp-lenses with text. The indicators represent the sensors of the systems; deviations from the desired value of a sensing-point are indicated by a lighted lamp-lens. The indicators have been functionally arranged on the panel surface. Push-buttons are used as controls; they are functionally arranged on the horizontal panel surface. More details about the lay-out of this TCC are described in earlier publications (1,2).

In the late seventies those technological developments had made such great progress that it became possible to use computers and VDU's in the TCC. Therefore a further reduction of running costs, still desired by the navy, could again be realised by an increase in the level of automation and a decrease of ship's complement. How to use these new technologies in the TCC on the last four Kortenaer-class frigates to be built, has been examined by a working group consisting of representatives from navy, ship-yard and Institute for Perception TNO. The main result of this pilot-study showed that application of the new technology on these frigates was possible in principle, but that much research still had to be done in the field of presentation of information on VDU's. The introduction of a new control and surveillance system would also require a considerable adaptation of operator training programs (3). Mainly because of the narrow time planning this so-called Adapted Technical Centre has never been realised on the Kortenaer-class frigates.

In this paper the Institute for Perception's part in the design and evaluation of a man-machine interface for supervisory and manual control of the technical systems on board the Walrus-class submarines will be discussed. Although this interface was developed in the first place for this new class of submarines, the technics and philosophies applied here are also applicable to surface ships. It has now been decided that the M-class frigates, put out to contract recently, will be provided with a control and surveillance system similar to that on the Walrus-class submarines. The system on board submarines will only differ from that on board surface ships with regard to a number of subsystems that are specific for submarines (e.g. balance control when being submerged). In addition there are higher demands for safety and redundancy in some aspects of submarine control.

Because the RNN has no special ergonomic branch or department, the Institute for Perception provides the ergonomic information and expertise needed in new building projects. In the main this advice is restricted to the most important workspaces on board naval ships (bridge, commmand centre, and technical centre). The institute is one of the four laboratories in the Defense Research Organization, a main research group of the TNO Organization (Organization for Applied Scientific Research). The Defense Research Organization is juridically independent of the Defense Department, though heavily subsidized by it. The laboratories develop their own research programmes for 5 years, which are annually discussed by a board of supervisors,among others consisting of representatives of the armed forces (Navy, Army, Air Force). By this organization the Institute for Perception TNO is able to take a relatively independent position in a project group consisting of the Navy, contractors and sub-contractors. From this position the institute gives its ergonomic advice to the RNN.

LAY-OUT OF THE TECHNICAL CONTROL CENTRE

The TCC on board the M-class frigates will have the same lay-out as the ones on the Tromp- and Kortenaer-class frigates: at the front bulk-head a row of panels to control and survey the technical systems and a row of consoles to coordinate the actions in the TCC and to communicate with the other technical rooms. Most of the actions will be done by means of VDU's. Between one and three operators (depending on the level of preparedness) are working at the panels, that are divided into electrical power generation and supply, propulsion control and ship's safety control. The consoles are unmanned under normal conditions at sea; only at higher levels of preparedness two officers will man them. The control and surveillance system is based on that of the Walrus-class submarines.

On the Walrus-class submarines the TCC is a part of the Combat Centre, from where sensor and weapon control and steering control also takes place. Figure 1 gives an overview of the lay-out of the Combat Centre on board the Walrus-class submarines.

At port side control and surveillance of the technical systems is situated. Therefore this panel, the Central Control Panel (CCP), forms the TCC on this type of submarines. At the front bulk-head the Steering Control Panel is situated.

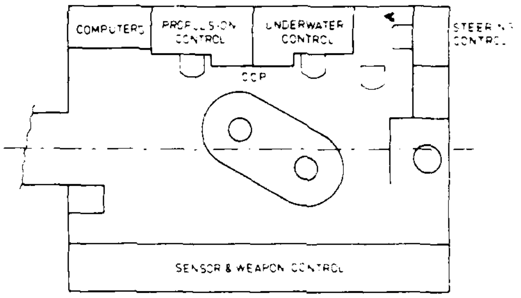


Fig. 1 Lay-out of the Combat Centre on the Walrus-class submarines.

Sailing at surface only the operators at the Propulsion Control Panel, the Steering Control Panel and some personnel for navigation are present. Sailing in submerged condition both control positions at the CCP and the helmsman's position are manned. Behind the helmsman and the operator at the Underwater Control Panel a supervisor (an experienced petty-officer) is sitting to coordinate the actions at the CCP and the Steering Control Panel and to keep contact between these operators and the commanding officer.

Because of the many VDU's in the control centre the illumination is adapted to this situation. During operations at sea the panels are illuminated by special luminaires that illuminate only an accurately adjustable part of the panel. This illumination can be dimmed over a big range so that the level of illumination in the Combat Centre can be adapted to the operational circumstances (e.g. the use of periscopes). When in harbour the Combat Centre is illuminated by fluorescent tubes.

LAY-OUT OF THE PANELS

The CCP has been divided into a Propulsion Control Panel (left) and an Underwater Control Panel (right). Both positions have a monocolour alpha-numeric VDU, a colour VDU and a functional keyboard with a trackball belonging to it. In addition a number of functional push-buttons has been located on the panel. Figure 2 shows the lay-out of the Propulsion Control Panel.

The CCP can be divided into four control surfaces. On the horizontal surface the functional keyboard and the trackball are located. With those devices the operator can call up information on both VDU's and, on the colour VDU, he can execute control actions with most of the ship's systems. On the first vertical surface the push-buttons that are used most frequently, and the colour VDU's are located. The second vertical surface includes the alpha-numeric VDU's and the push-buttons that are used less frequently. The upper vertical surface includes only emergency controls, indicators and displays.

Groups of push-buttons that belong together functionally are located within dark green rectangles. The background of the CCP has been coloured light green. These shades of green have been chosen so that even with a very low level of illumination the various groups of push-buttons still are distinguishable. The push-buttons themselves are coloured white. In some push-buttons an indicator (a LED) is fitted. Above each push-button its function has been written in white text

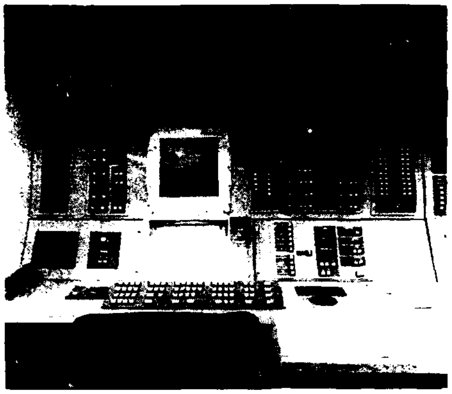


Fig. 2 Lay-out of the Propulsion Control Panel on the Walrus-class submarines.

that is illuminated internally. This illumination can be dimmed dependent on the operational circumstances.

On the CCP one can distinguish three control levels (see Fig. 3):
1. Automatic control
2. Remote manual conirol
3. Local manual control

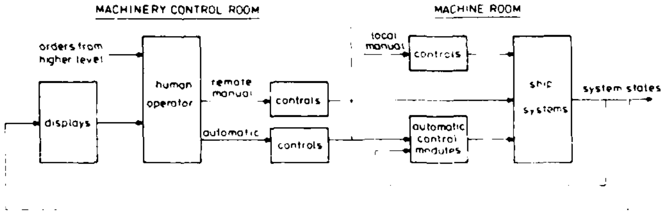


Fig. 3 Block diagram of the human operator task in the Technical Control Centre.

In normal conditions the most important systems will be controlled by Automatic Control Modules (ACM's). The operator wi;l act as a supervisor of those systems (level 1) and he may have to change the setpoint of an ACM. By looking at the process schemes of the systems he can monitor this actual state and, over a lorg time, try to build up internal representations of the systems. In some special circumstances, for example a fault in the ACM or if the operator wants to perform an action that is not incorporated in the ACM, he has to take over control manually. In that case it is preferable to control the systems remotely from the TCC

(level 2), but if that is not possible someone has to go to the machine room to control them locally (level 3).
Working at control level 2 the operator uses the colour VDU, the trackball and the functional keyboard. These actions will be discussed more extensively below.

DESIGN EVALUATION TECHNICS

A number of design evaluation techniques were used during the design process of the CCP. Based upon data provided by the RNN on the number of operators and their tasks the dimensions of the CCP were defined on paper, taking into account anthropometric data and space needed for maintenance. After this phase a complete scale 1:1 mock-up of the Combat Centre was built in wood. The front surface of the CCP was covered with flannel in order to define the lay-out. Taking into account the interactions between human operators and apparatus this lay-out was defined by a committee consisting of representatives from the Navy (including the future users), manufacturers and the Institute for Perception TNO. After a freeze-point for the main parts the CCP in the mock-up was made in its ultimate form with every detail included (see Fig. 2).

To evaluate the lay-out of the CCP in this phase, two teams consisting of four experienced submariners played a role-play in the (static) mock-up. Both teams executed four exercises that covered a large part of the tasks in the CCP. This experiment yielded data on information that was missing or was poorly visible, some illogical control sequences and some controls that were hardly within reach for small operators. Moreover this experiment was a good introduction of the new control and surveillance system to the future users (4). However, in a static simulation the use of and the interaction with the VDU's is left completely out of consideration. That's why for some tasks a number of dynamic experiments have been carried out.

Which input device would be optimal in the task situation at the CCP was tested in an experiment. Results showed that the trackball would be the best (5).
In another experiment the optimal transfer function between trackball and cursor on the colour VDU was defined. Dependent variables were the time to mark a target and the number of errors made. The dimensions of the smallest target that did not result in a higher error rate were defined as well(6).
Which hand should control the trackball and the keyboard respectively was tested too, given the lay-out of the keyboard chosen for the Walrus. It is mainly the right part of the keyboard which is used in combination with the trackball. Controlling the trackball with the left hand and the keyboard with the right hand resulted in the best performance.
A comparison of two presentation principles for process schemes on the colour VDU was also carried out. The tasks in this experiment covered both the recognition of the system state and the performance of a control order. In the next paragraph this experiment will be discussed more extensively.

The experiments described above cover only a small part of the complete operator task. Moreover, only normal conditions were taken into account. Therefore a simulator will be built to do research on operator performance under both normal and abnormal conditions. On this simulator future crew members can be trained as well. To support the simulator research a group of experienced submariners and submarine designers filled in a questionnaire with questions on the frequency of occurrence and the seriousness of a large number of calamities. By computing the product of seriousness and frequency of occurrence the calamities could be ranked from rare and not serious to frequent and very serious. This list of calamities will play a role in setting up training programs and defining scenario's for research.

On the M-class frigates some new design techniques will be used in the design process of the TCC. At the moment the project is still in the pre-design phase:

there are navy specifications and some preliminary drawings. A wooden mock-up of the TCC has not yet been built. Computer Aided Design (CAD) techniques will be used to define the lay-out of the TCC, the panel dimensions and the rough lay-out of the panels. This phase is considered as a preparation for the mock-up phase. By using CAD-technics the (expensive) mock-up will hopefully have to be modified less frequently. To analyse operator tasks, interactions between operators and interactions between operators and apparatus analytical models (e.g. SAINT) will be used (7). With this tool bottlenecks in the operator task can be identified so that modifications in the design can be introduced at an early stage of the project.

INFORMATION PRESENTATION ON THE VDU'S

The top VDU is used to present a list of alarms. In this list the time of occurrence, a description of the sensing-point and the higher and lower limits of the sensing-point are given for each alarm. If the list of alarms is too long to present on one page, a window can be moved over the list to present the desired part. A newly occurring alarm is indicated by a blinking pointer on the alpha-numeric VDU in combination with an auditory signal. After the operator has accepted the alarm, the auditory signal disappears and the pointer is displayed steadily. On this VDU a list of inhibited sensors can also be presented.
The Navy requires that this VDU will work under all environmental conditions, as long as the computer system is operating. These are requirements that only milspec VDU's can satisfy. Therefore a plasma display has been selected that has the additional advantage that a lot of data can be presented on one page (8).

For the colour VDU less severe requirements with respect to resistance against environmental influences are in force. If the colour screen drops out and the computer system, the alpha-numeric VDU and the functional push-buttons of the ACM's and the direct controls are still operating, then the systems can be controlled and surveyed in a way that is acceptable to the RNN. Therefore ruggidized civil equipment has been chosen as a colour VDU and graphic processor belonging to it.

The colour VDU is used for two purposes: as a display for various types of data and as an interactive control device. On this device process data can be called up in the form of process schemes, trend diagrams and general data on systems and components. For almost every system a process scheme is available; some small systems are presented in combined schemes. The process schemes give an image of system construction by presenting the configuration of pumps, valves, pipelines, etc. During the design process of these schemes the aim was to present the system function as well as possible. This resulted in a presentation that was not always in accordance with the real (topographic) situation in the ship. This topic will be discussed more extensively below.

In the process schemes the actual value of sensing-points, the state of pumps, valves, switches, etc. (e.g. opened/closed, on/off) and the presence of a pressure or flow in a pipeline are presented. The last two items are shown as two shades of the same colour. In addition to the presentation of the actual system state, the process schemes are also used to execute control actions: the operator selects an element in the scheme by means of a trackball controlled cursor and then types in a command string on the functional keyboard. In that way he has to control all the elements needed to complete his intended action. The results of his actions are, after some delay, presented in the process scheme. Using this procedure it is not necessary to type in an identification code for each element (with a high error probability), and in the process schemes no identification codes have to be presented, resulting in a better surveyability.

The operator also has at his disposal trend diagrams of a number of variables. The operator is free to define a part of these trends. At this moment no ultimate decision has been made on the way trend diagrams will be presented on the colour VDU (e.g. dimensions, ratio between amplitude and time-base). In a recent experiment White and van Heusden examined to what extent operators could predict a limit crossing of a variable, depending on various display scalings (9). The results of this experiment give a sufficient starting-point for making an acceptable choice.

A comparison of two different display structures

In the last paragraph we already mentioned that in the presentation of the process schemes it is the system function which is emphasized (functional structure). This means that the topographic configuration of the systems (e.g. connections between valves, pumps, pipelines) will not always be so obvious. Discussing the design of the process schemes in the system design group, consisting of engineers and submarine personnel, it became clear that the two groups had different opinions.

The system engineers thought that operators will perform better if the functional structure of a system is presented in the process scheme in an unambiguous way, and that the topographical structure is less important in a remote control situation. Most of the systems are so complicated that it is impossible to present the topographic structure in one picture on the colour VDU; so one always has to make a compromise. Another consequence of a topographic presentation can be the occurrence of crossing pipelines, loops in pipeline systems and a contrast of the overall flow direction with the direction a pump is pointing to. These disadvantages can often be avoided when priority is given to the presentation of the functional structure of the system.

On the other hand the submarine personnel strongly preferred process schemes in which the topographic structure of the systems is presented as accurately as possible. On the submarines now in use with the RNN, and in which they have sailed for several years, most of the systems are controlled locally and manually. They have built up a fairly good internal representation of the physical structure of the systems, and they want to recognise this representation in the process schemes. Moreover they are afraid that they cannot control the systems locally any more if they have only worked with process schemes built up according to the functional structure of the systems.

Given these considerations one can pose the following questions:

1. Will an experienced operator perform better with a functional presentation than with a topographic presentation?
2. Is there a difference between experienced and inexperienced operators?
3. Is there a difference in learning with the two presentations?

To answer these questions objectively, apart from the subjective opinions of designers and users, an experiment was set up with both experienced and inexperienced operators who had to control a simulated submarine system with two display structures. In this experiment two aspects of the supervisory task were incorporated, namely the recognition of a system state and the manual execution of a control order. The tasks were executed in the remote manual mode (see fig. 3) using a colour VDU, a trackball and a functional keyboard. Because we have already reported this experiment more extensively we will discuss it only briefly here (10).

In the experiment two display structures of the trim system of a submarine were used because of the limited complexity, the reasonable number of control possibilities and the fact that it is easy to explain to inexperienced subjects.
Ten inexperienced subjects (all staff of the Institute for Perception TNO) and ten experienced submariners (petty-officers) participated in the experiment. The inexperienced subjects only participated in a pilot-experiment with pencil and paper. In order to be able to compare the performance of experienced and inexperienced subjects, the submariners also participated in the pencil and paper experiment. After that they executed the same tasks with a colour VDU, a trackball and a keyboard. In the first part of the experiment they had to indicate in what direc-

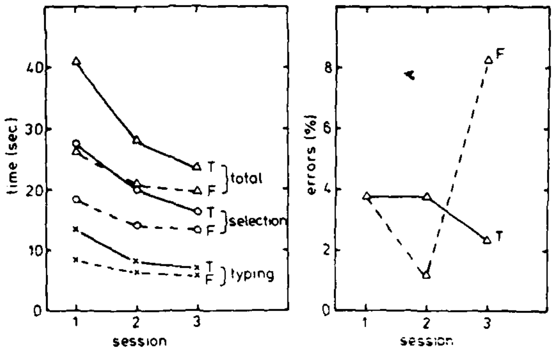


Fig. 5 Mean action time and mean error rate in the control order task as a function of session (T=topographical; F=functional).

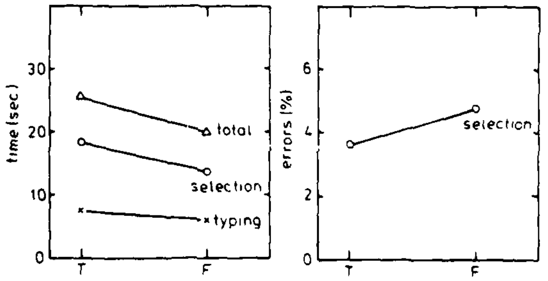


Fig. 6 Mean action time and mean error rate in the control order task for two display structures (T=topographic; F=functional).

Whenever there was some time left over we asked one or two subjects to do one control order task session with the other display structure; the other subjects who were present that day could watch this added session. Then we asked the subjects which display structure they preferred. All subjects chose the functional display structure, regardless of the structure they had practiced with, because they found this structure more surveyable. So during the experiment some subjects abandoned their initial rejection of the functional display structure and accepted it as a good and understandable presentation of a process-scheme.

From the results of this experiment one can conclude that subjects perform better with the functional display structure because of the better selection time. This effect occurs immediately but decreases with practice. Experienced submariners perform better than laymen (laboratory personnel). Finally an experiment simulating a well known practical situation is a much better way of convincing practical men than a long series of good arguments.

Based on the results of this experiment it is decided to give priority to the function of systems in process schemes. Nevertheless we will aim at presenting some important topographic aspects of the systems as well, as long as this will not affect the surveyability of the pictures.

CONCLUSION

Because of the rise of automation on naval ships, more and more tasks will be allocated to automatons. Therefore the nature of the operator's task will change more and more from active to passive watching, as the number of systems that has to be watched will increase. However, the operator's workload will then increase too, especially under abnormal conditions. These developments have been recognized earlier (12,13).

It is expected, however, that the application of VDU's in the TCC will increase in future. The workplace will then be composed of a number of VDU's, functional keyboard, trackball (or another input device) and a very limited number of push-buttons, indicators and displays. Then the question arises whether the operator will still be able to overview the system state sufficiently under all operational conditions. For on VDU's information is presented in a sequential form. Therefore, much attention has to be paid to the design of overview pictures (14).

Likewise, in the literature very little is known about the way information on VDU's should be categorized into a number of hierarchical levels (from overview information to detailed system information). Most authors only present some ideas that have not been tested at all in a (simulated) practical situation (15,16).

Another research item will be the design of the so-called operational pictures. On board naval ships a number of events will occur, to which the operator has to react in the first instance in a standardized way (e.g. fire alarm, big leakage). Because these actions usually have to be executed quickly, it will probably be useful for task performance to present in one operational picture all the information needed during that particular action. Ergonomic expertise will be indispensable in solving all these problems.
It appears, from various sources in the literature, that between 70 and 90 percent of all accidents in industry, transport systems and houses is caused by human errors (17). In many occasions these human errors are caused by a very high or a very low workload, errors in the design of the man-machine system, and wrong or not clearly formulated procedures. As the number of automatons increases and the automatons themselves become more reliable at the same time, the proportion of human errors will increase more and more. Therefore, the measurement of workload, in relation to integration and reduction of information and the allocation of tasks to man and machine, will increase in importance.

At this moment the RNN only has a training simulator for the TCC available on board the Tromp- and Kortenaer-class frigates. New crew-members get their basic training on this device. For the greater part team-training and refresh-training is done on board hip. The training of submariners is even done almost completely on board. Because it is difficult (and often not without risk) to simulate calamities in a standardized way on board, and because the complement on new types of ships will be too small to care for training themselves, training simulators will be necessary in near future. Most urgent in this context are good procedure simulators.

In general it can be stated that developments in the TCC point in the direction of an integrated workplace, built up around a number of VDU's. The analysis of panel lay-out by means of mock-ups will decrease in importance in favour of research to operator workload and presentation of information. It will be a challange to the ergonomists to anticipate these changes.

REFERENCES

(1) J. Brink and J.F.D. Kuypers, "Control and Surveillance of Ship Systems by means of VDU's and Digital Programmable Components", Proceedings of the 6th Ship Control Systems Symposium, Ottawa, Canada, 1981.

(2) H. Schuffel, "The Lay-out of the Technical Control Centre for the Standard Frigates of the Royal Netherlands Navy" (in dutch, abstract in english), Institute for Perception TNO, Soesterberg, NL, report nr. IZF 1983-28, 1983.

(3) J. Vermeulen, "Pilot-study to the possibilities of an Adapted Technical Centre (ATC) on the Standard Frigates" (in dutch, abstract in english), Institute for Perception TNO, Soesterberg, NL, report nr. IZF 1982-38, 1982.

(4) J. Vermeulen, "Evaluation of the Central Control Panel (CCP) of the Walrus-class Submarines by means of a Static Simulation in the Mock-up" (in dutch), Institute for Perception TNO, Soesterberg, NL, report nr. IZF 1982-M30, 1982.

(5) P.T.W. Hudson, "Computer Compatible Display Devices: A Study of Optimalised Devices with Static and Moving Targets", Institute for Perception TNO, Soesterberg, NL, report nr. IZF 1982-4, 1982.

(6) J. Vermeulen, "Selecting of Elements in Process Schemes on a CRT - A Comparative Study between Four Types of Trackballs" (in dutch, abstract in english), Institute for Perception TNO, Soesterberg, NL, report nr. IZF 1984-4, 1984.

(7) D.J. Seifert und B. Döring, "SAINT - A Technique for Modelling, Simulation and Analysis of Man-machine Systems" (in german, abstract in english), Angewandte Systemanalyse Band 2 (Heft 3), 1981.

(8) J. Vermeulen, "Some Aspects of Using the Alpha-numeric Display in the Central Control Panel (CCP) of the Walrus-class Submarines" (in dutch, abstract in english), Institute for Perception TNO, Soesterberg, NL, report nr. IZF 1982-33, 1982.

(9) T.N White and A.R. van Heusden, "Various Display Scalings of Trend Information and Human's Predictability", 4th European Annual Conference on Human Decision Making and Manual Control, Soesterberg, NL, may 1984.

(10)J. Vermeulen, "The Effects of Display Structure on Supervisory Control of Ship Systems", 3rd European Annual Conference on Human Decision Making and Manual Control, Roskilde, DK, may 1983.

(11)J.B. Brooke and K.D. Duncan, "Effects of Prolonged Practice on Performance in a Fault Location Task", Ergonomics, 26, 4, 1983, pp. 379 - 393.

(12)T.B. Sheridan and G. Johannsen, "Monitoring Behaviour and Supervisory Control", Plenum Press, London, 1976.

(13)E.L. Wiener and R.E. Curry, "Flight-deck Automation: Promises and Problems", Ergonomics, 23, 10, 1980, pp. 995 -1011.

(14)J.H. Poessé, J.E. Rijnsdorp and T.N. White, "Evaluation of Overview Pictures for Process Supervision", 4th European Annual Conference on Human Decision Making and Manual Control, Soesterberg, NL, may 1984.

(15)L. Bainbridge, "Ironies of Automation", IFAC Conference on Analysis, Design and Evaluation of Man-machine Systems, Baden-Baden, FRG, sep. 1982, pp. 151 -157.

(16)L.P. Goodstein, "An Integrated Display Set for Process Operators", IFAC Conference on Analysis, Desig and Evaluation of Man-machine Systems, Baden-Baden, FRG, sep. 1982, pp. 75 - 82.

(17)W.A. Wagenaar, "Human Failure" (in Dutch), Inaugural address, University of Leiden, NL, feb. 1983.